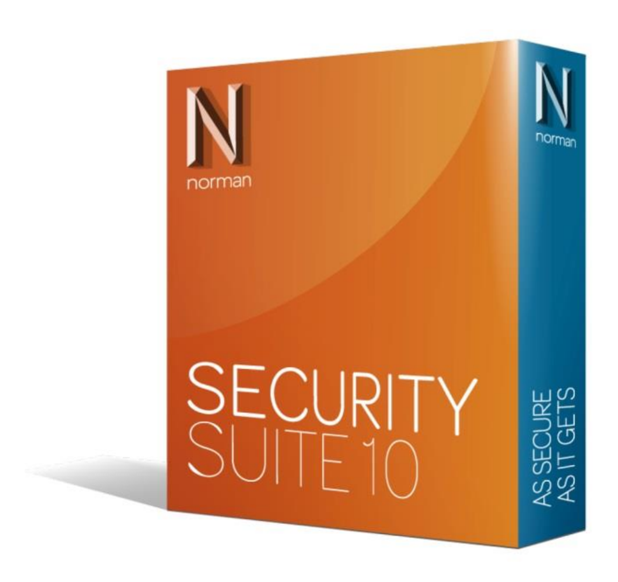


Security Suite

Benutzerhandbuch

Norman Security Suite



- Installation
- Erste Schritte
- Erklärung der einzelnen Komponenten
- Aktualisierungen
- Support
- Deinstallation

NORMAN DATA DEFENSE SYSTEMS GMBH
GLADBECKER STR. 3
40472 DÜSSELDORF
TEL: +49 (0) 211 586 99 0

NIEDERLASSUNG MÜNCHEN
LUDWIGSTR. 47
85399 HALLBERGMOOS
TEL: +49 (0) 811 541 84 0

INFO@NORMAN.DE WWW.NORMAN.DE



Inhalt

Einführung ... 4
Systemvoraussetzungen ... 4
Informationen zu dieser Version ... 4
Informationen zu diesem Handbuch ... 4
Schulungen und technische Unterstützung ... 4
Was ist die Norman Security Suite? ... 5
Virenschutz ... 5
Persönliche Firewall ... 6
Spamschutz ... 7
Jugendschutz ... 7
Datenschutztools ... 7
Eindringschutz (Englisch Intrusion Guard) ... 8
Installation ... 9
Abrufen der Software ... 9
Lizenzschlüssel ... 10
Installation läuft ... 10
Assistenten ... 11
Installationsassistent ... 12
Erste Schritte ... 13
Anwendungssymbol in der Taskleiste ... 13
Warnsymbole in der Taskleiste ... 13
Öffnen der Anwendung ... 14
Einstellungen der Security Suite ... 15
Security Suite Startseite ... 16
Virenschutz ... 17
Pausieren bzw. deaktivieren des Automatischen Scanners: ... 17
Einstellungen Ändern ... 17
Automatischer Scanner ... 18
Manueller Scanner ... 20
Weitere Prüfverfahren ... **21**
Kontextmenü-Scanner ... 21
Befehlszeilen-Scanner ... 21
Quarantäne ... 22
Aufgaben-Editor ... 23
Ausschlussliste ... 24

Persönliche Firewall 26
Einstellungen anpassen 26
Persönliche Firewall konfigurieren 26
Erweiterte Einstellungen 27
Profi-Werkzeuge 27
Regelassistent 27
Regel anlegen: 28
Dienstprogramm für Echtzeitprotokoll 28
Erweiterte Port-Anzeige 28
Personal Firewall deaktivieren / aktivieren oder deinstallieren 30
Spamschutz 31
Einstellungen anpassen 31
Sperren/Zulassen 32
Einstellungen 33
Jugendschutz 34
Benutzer 34
Standardprofileinstellungen 35
Benutzer anlegen 36
Administratorkennwort ändern 37
Datenschutztools 38
Programmverlauf eines Benutzers löschen 38
Sicher löschen 38
Eindringschutz (Englisch Intrusion Guard) 39
Treiber und Speicher 39
Prozesse 40
Vertrauenswürdige Prozesse 40
Netzwerk 40
Softwareupdate 41
Proxy eintragen: 41
Produktsprache auswählen 41
Lizenzassistent (Lizenz eintragen) 41
Support Center 42
NSS deinstallieren 43
Anhang A 44
Was ist eine Sandbox? 44

Einführung

Systemvoraussetzungen

Diese folgenden Betriebssystem Versionen unterstützen die Installation der Norman Security Suite Version 10.1 auf Computern mit den Betriebssystemen Windows XP, Windows Vista, Windows 7 und Windows 8/8.1 entsprechend den folgenden Spezifikationen:

Windows		**XP**	**Vista**	**7**	**8 / 8.1**
Antivirus		👍	👍	👍	👍
Intrusion Guard		nur 32 Bit	👍	👍	👍
Personal Firewall			👍	👍	👍
Parental Control			👍	👍	👍
Antispam 1)			👍	👍	👍
Privacy Tools			👍	👍	👍
Service Pack	oder höher	2	1	1	
Prozessor (Pentium-basiert)	Empfohlen	1,8 GHz			1,8 GHz
RAM	Empfohlen	2 GB			2 GB
Freier Speicherplatz auf Festplatte	Empfohlen	2 GB			2 GB
Bildschirmauflösung	Empfohlen	1024x768			1024x768

1) Antispam ist nur für Windows Outlook, Outlook Express und Vista Mail verfügbar.

Eine aktuelle Übersicht der Voraussetzungen finden Sie unter:
http://safeground.norman.com/de/home_and_small_office/systemanforderungen

Informationen zu dieser Version

Das aktuelle Release steht in mehreren Sprachen zur Verfügung. Es wird in unregelmäßigen Abständen um neue Sprachen erweitert. Wenden Sie sich an Ihren Norman-Vertragshändler, wenn Sie Informationen zur Security Suite in Ihrer Sprache benötigen. Detaillierte Informationen hierzu finden Sie auf der Website von Norman. Sie können sich aber auch an Ihren lokalen Händler wenden, wenn Sie weitere Informationen zu Sprachversionen wünschen.

Informationen zu diesem Handbuch

In diesem Handbuch werden Produkte, Merkmale und Hauptfunktionen der Norman Security Suite im Überblick dargestellt. Eine ausführliche Beschreibung aller verfügbaren Optionen finden Sie in der Onlinehilfe.

HINWEIS: Besondere oder wichtige Hinweise sind mit einem Ausrufezeichen am linken Rand gekennzeichnet.

Schulungen und technische Unterstützung

Mit Anfragen zu Schulungen und technischer Unterstützung wenden Sie sich bitte an Ihren Händler vor Ort oder an Norman ASA. Norman bietet technische Unterstützung und Beratung zur Security Suite und zu allgemeinen Sicherheitsfragen an. Die technische Unterstützung beinhaltet zudem die Gewährleistung der Qualität Ihrer Antivireninstallation, einschließlich Unterstützung bei der Anpassung der Security Suite an Ihre Anforderungen. Beachten Sie, dass der Umfang der angebotenen Dienstleistungen je nach Land variiert.

Kontaktangaben zu Niederlassungen von Norman finden Sie auf der letzten Seite des Handbuchs.

Was ist die Norman Security Suite?

Die Norman Security Suite (NSS) ist ein Softwaresicherheitspaket, das sich aus sechs verschiedenen Sicherheitsanwendungen zusammensetzt:

Virenschutz	Verhindert das Eindringen von Viren in den Computer
Persönliche Firewall	Verhindert den Missbrauch Ihres Computers als Transit für unerwünschten Datenverkehr durch Hacker
Spamschutz	Blockiert unerwünschte SPAM und Massen-E-Mails
Jugendschutz	Verhindert den Besuch von Kindern auf Websites mit ungeeigneten Inhalten
Datenschutztools	Sorgt für sicheres Löschen von Dateien und persönlichen Daten.
Eindringschutz	Verhindert das Eindringen bösartiger Programme in Ihren Computer

* Die beiden letzten Anwendungen – Datenschutztools und Eindringschutz – sind nur in der Version Security Suite PRO enthalten.

Die Norman Security Suite ist nach der Installation sofort einsatzbereit. Die standardmäßigen Konfigurationseinstellungen bieten den benötigten Schutz. Sie müssen sich nicht durch sämtliche Konfigurationsoptionen kämpfen, um das Programm zum Laufen zu bringen. Dennoch ist es hilfreich, eine Vorstellung davon zu haben, wie das Programm funktioniert, und sich mit den Grundfunktionen vertraut zu machen. In diesem Handbuch wird auf bestimmte hilfreiche Funktionen hingewiesen, und es werden Tipps gegeben, mit deren Hilfe sich das Programm optimal einsetzen lässt.

Virenschutz

Dieses Virenschutzprogramm scannt Ihren PC auf Schadsoftware (Malware). Bei Malware handelt es sich um Computerviren, -würmer, Trojaner und sonstige unerwünschte Codes. Spyware entfaltet keine zerstörerische Wirkung wie herkömmliche Viren. Die unerwünschte Offenlegung persönlicher Daten kann jedoch ebenso großen Schaden anrichten. Die einzigarte Sandbox von Norman bietet proaktiven Schutz –und das sogar vor unbekannten Viren

Weitere Informationen zur Sandbox finden Sie auf Seite „Anhang A“ auf Seite <?>.

Viren lassen sich automatisch von Festplatten, Wechselmedien, aus E-Mail-Anhängen usw. entfernen. Die Virenschutz-Anwendung prüft Dateien beim Öffnen und entfernt möglicherweise vorhandene Viren automatisch. Die Security Suite beinhaltet zwei Hauptscanner – den automatischen Scanner und den manuellen Scanner – sowie diverse andere Scanverfahren.

Wir empfehlen, den Computer gelegentlich auch manuell zu prüfen. Über das Taskleistenmenü können Sie den gesamten Computer überprüfen lassen – und zwar spontan. Ferner können Sie mithilfe des Kontextmenüs beim Durchsuchen von Ordnern einzelne Dateien prüfen oder Normans Bildschirmschoner aktivieren, wodurch ebenfalls eine Virenüberprüfung in Gang gesetzt wird. Wenn Sie die Arbeit fortsetzen, wird die Prüfung abgebrochen und bei der nächsten Aktivierung des Bildschirmschoners an derselben Stelle wieder aufgenommen. Regelmäßige manuelle Prüfungen können Sie mit dem Aufgaben-Editor und Zeitplaner einrichten. Dort können Sie auch festlegen, welcher Bereich des Computers wann geprüft werden soll.

Dieses Produkt wird mit vorkonfigurierten Einstellungen geliefert, die ausreichen sollten, um Ihren Computer vor Virenangriffen zu schützen. Die Module können Sie jedoch so konfigurieren, dass die jeweilige Anwendung Ihren individuellen Anforderungen genügt.

Persönliche Firewall

Immer wenn Sie mit dem Internet verbunden sind, E-Mails lesen oder im Web surfen, stellen Sie Verbindungen zu Computern auf der ganzen Welt her – und diese zu Ihnen. Und da fangen die Probleme an. Wenn Hacker in Ihren Computer eindringen, können sie auf Ihre privaten Dokumente zugreifen, Ihren Computer für ihre eigenen Zwecke missbrauchen oder ihn sogar völlig nutzlos machen, indem sie wichtige Systemdateien löschen.

Die vorliegende Anwendung dient in erster Linie dem Schutz vor Hackerangriffen und kontrolliert daher den eingehenden und ausgehenden Datenverkehr Ihres Computers gemäß einer Sicherheitsrichtlinie (einem Regelsatz). Diese Regeln werden (automatisch oder benutzerspezifisch) beim Installieren des Produkts festgelegt.

Der Regelassistent der Anwendung kann automatisch Regeln für den Internetzugriff der Anwendung erstellen. Es gibt unterschiedliche Modi für erfahrene und unerfahrene Benutzer, und die Anwendung kann sogar den Servermodus erkennen. Zudem können Sie Regeln erstellen und ändern sowie Details zum Datenverkehr und der Aktivität der Ports anzeigen.

Daneben bietet die erweiterte Persönliche Firewall folgende Funktionen:

Schutz vor getarnten Starts (Stealth Launch Protection), der bösartige Anwendungen enttarnt, die versuchen, über andere Anwendungen auf das Internet zuzugreifen. Die Personal Firewall verfolgt alle übergeordneten Anwendungen.

Volltarnmodus (Full Stealth Mode), der sicherstellt, dass alle Ports Ihres Computers von außen unsichtbar sind.

Erweiterte svchost-Verwaltung, bei der für jeden svchost-Dienst gesonderte Regeln gelten statt einer allgemeinen Regel für die Gruppe von Diensten, die in jeder Sitzung der svchost.exe enthalten sein kann.

Svchost ist ein generischer Hostprozess für Dienste unter Windows XP/2003/Vista/7/8, der für die ordnungsgemäße Ausführung diverser Netzwerk- und Internetprozesse erforderlich ist. Dieser Dienst kann viele Instanzen gleichzeitig ausführen, die jeweils für den Betrieb der einzelnen Computer notwendig sind. Der Dienst ist berechtigt, häufig auf das Internet zuzugreifen, und wird wie jede andere Anwendung, die sich mit dem Internet verbindet, von der Firewall überwacht. Diese gibt bei verdächtigen Aktivitäten eine Warnung aus. Während viele Firewalls nur über eine einzige allgemeine Regel für den Umgang mit svchost verfügen, die sich noch dazu meist nicht bearbeiten lässt, unterscheidet diese Firewall zwischen unterschiedlichen Instanzen und erkennt, ob der Prozess bekannt oder unbekannt ist. Daneben finden sich in den Hilfedateien der Anwendungen Konfigurationsoptionen für eine Reihe von svchost-Diensten.

!!! HINWEIS: Standardmäßig hat die Persönliche Firewall 3 Operationsmodies, welche in der Norman Security Suite Oberfläche unter dem Punkt „Einstellungen" „Persönliche Firewall Konfiguration" (Kleines Stiftsymbol neben „Persönliche Firewall" auf der rechten Seite) geändert werden können. :

Unbeaufsichtigter Modus: Die persönliche Firewall lässt allen Datenverkehr zu, der nicht durch eine spezielle Regel blockiert wird. Sie ist im Hintergrund unbemerkt aktiv und schützt ohne jegliche Benutzereingriffe gegen Angriff von außen.

Normaler Modus: Dieser Modus ist per default ausgewählt. Bei unbekannten Datenverkehr wird sofort eine Eingabeaufforderung eingeblendet. Es wird ein Popup mit Details zu der Anwendung angezeigt, die den Netzwerkzugriff versucht. Mithilfe von permanenten oder nur für die aktuelle Sitzung gültigen Regeln können Sie festlegen, ob der Verkehr zugelassen oder verweigert werden soll. Somit sind Sie sowohl gegen Angriffe von außen als auch gegen das unerwünschte Versenden Ihrer Daten durch Anwendungen auf dem Computer geschützt.

Erweiterter Modus: Diese Firewall-Operation entspricht im Wesentlichen dem normalen Modus, allerdings wird die DPI-Funktion (Deep Process Inspection) standardmäßig aktiviert. Die DPI-Funktion bietet erweiterten Schutz gegen Trojanerangriffe, bei denen versucht wird, Daten durch die Firewall zu schmuggeln. Die Protokollierung ist detaillierter und umfasst eine vollständige Aufstellung aller Dienste, die im Kontext einer SVchost.exe- Sitzung ausgeführt werden. Da die DPI-Funktion viele Ressourcen in Anspruch nimmt, wird sie aus Leistungsgründen für langsamere Computer nicht empfohlen. Aufgrund dieser Leistungseinbußen kann es möglicherweise auch zu Kompatibilititäsproblemen mit Anwendung von Drittanbietern kommen. Das liegt daran, dass der Paketempfang einige Millisekunden länger dauern kann, sodass in einigen Fällen das erste an die Anwendung gesendete Paket verlorengeht (und erneut gesendet werden muss). Wenn bei einer Ihrer Anwendungen solche Probleme auftreten, können Sie die DPI-Funktion über eine Regel im erweiterten Regelassistenten deaktivieren.

Spamschutz

Die Spamschutz-Anwendung schützt vor unerwünschten Werbe- und Massensendungen per E-Mail (sogenanntem „Spam“), die u. U. eine Bedrohung für das System darstellen. Antispam blockiert Spam, Phishing-Angriffe und sonstige E-Mail-Bedrohungen, bevor sie Ihren Computer erreichen. Mithilfe von Sperr- und Zulassungslisten können Sie selbst bestimmen, von wem Sie E-Mails annehmen und welche Inhalte zum E-Mail-Client weitergeleitet werden dürfen.

So wie Antiviren-Anwendungen mit Virendefinitionsdateien arbeiten, um Malware zu erkennen, verwenden Antispam-Lösungen Definitionsdateien, um unerwünschte E-Mails herauszufiltern. Virendefinitionsdateien nutzen Virensignaturen, um zu ermitteln, ob eine bestimmte Datei infiziert ist, wohingegen Antispam-Definitionen mithilfe eines bestimmten Kriteriensatzes ermitteln, welche E-Mails vermutlich Spam beinhalten. Spam-Definitionsdateien analysieren E-Mails anhand von Sprache, Bildern, Farben, Hyperlinks, die die Mail enthält, sowie anhand der Absender- und IP-Adresse. Trotzdem lässt sich nicht mit letzter Sicherheit sagen, ob es sich bei einer vorliegenden E-Mail um Spam handelt oder nicht.

Spam

Unter Spam versteht man unerwünschte E-Mail, normalerweise Produktwerbung. Spam ist meist harmlos, kann aber lästig und zeitraubend sein.

Phishing

Als Phishing bezeichnet man das Versenden von E-Mail unter dem Vorwand, ein seriöses öffentliches oder privates Unternehmen zu sein, um Privatinformationen zu erschleichen und somit Identitätsdaten zu stehlen. In solchen E-Mails werden Sie beispielsweise aufgefordert, persönliche Informationen wie Kreditkarten- oder Kontonummern zu aktualisieren, also Informationen, die den echten Unternehmen längst vorliegen. Die Websites sind nachgestellt, sehen aber oft täuschend echt aus und dienen ausschließlich dem Zweck, Daten zu stehlen. Der Begriff „Phishing“ selbst ist vom englischen Wort für „Fischen“ abgeleitet und bemüht das Bild von Köder und Haken, denen der Empfänger solcher Angriffe gleichsam zum Opfer fällt.

Jugendschutz

Das Internet ist nicht unbedingt ein sicherer Ort. Zudem gibt es Websites, die Kinder lieber nicht zu sehen bekommen sollten. Sofern wir das Surfverhalten unserer Kinder und Teenager nicht ständig überwachen, besteht die Möglichkeit, dass diese gewollt oder ungewollt Websites mit gefährlichem oder obszönem Inhalt aufrufen.

Mit dem Kinder- und Jugendschutz können Sie den Zugang zu Websites bestimmter Kategorien unterbinden und sogar alle Sites blockieren, die Sie nicht ausdrücklich genehmigt haben. Darüber hinaus können Sie die Zeit beschränken, die ein Benutzer im Internet surfen darf, und festlegen, zu welchen Tageszeiten dies erlaubt ist.

Kurz gesagt können Sie auf der Basis des Alters oder anderer zu berücksichtigender Kriterien für den einzelnen Benutzer ein persönliches Nutzungsprofil anlegen.

Datenschutztools

Viele Anwendungen, darunter auch das Betriebssystem selbst, protokollieren Benutzeraktivitäten, also z. B. welche Dateien geöffnet, welche Websites besucht und welche Dokumente aufgerufen wurden. Es handelt sich dabei um einen benutzerfreundlichen Mechanismus, der wiederkehrende Aufgaben bequemer macht, etwa den Besuch der selben Onlinezeitung oder die Weiterbearbeitung einer Textdatei.

So benutzerfreundlich dies sein mag, ergibt sich ein Datenschutzproblem. Andere Benutzer desselben Computers oder Personen, die Ihren Computer zu einem späteren Zeitpunkt prüfen, können Einsicht in diese Protokolldateien nehmen und Dinge entdecken, die möglicherweise vertraulich sind. Auch das Löschen von Dateien entfernt nicht alle Spuren. Fortgeschrittene Tools können gelöschte Dateien wiederherstellen und die Sicherheit sensibler Dokumente gefährden. Protokolle verfolgen Internetsuchen und Dateien, die Sie auf Ihrem Computer öffnen.

Diese Funktion hat enorme Bedeutung für Ihren Datenschutz. Denn sie birgt das Risiko des Social-Engineering und Identitäts- und Kennwortdiebstahls. Die angeeigneten Privatinformationen können wiederum missbraucht werden.

Die Norman Security Suite Datenschutztools ermöglichen Ihnen, bestimmte Dateien sicher zu löschen. Die Inhalte solcher Dateien sind dauerhaft gelöscht und lassen sich nicht wiederherstellen. Sie können die Anwendung auch so konfigurieren, dass diverse Protokolldateien mit persönlichen Daten, Cookies und Browserverläufen automatisch gelöscht werden. Das Löschen von Verlaufsprotokollen wirkt sich nicht auf die Einstellungen und Lesezeichen einer Anwendung aus.

Eindringschutz (Englisch Intrusion Guard)

Dies ist ein hostbasiertes Intrusion Prevention System (HIPD), mit dem schädliche Anwendungen davon abgehalten werden, die Kontrolle über Ihren Rechner zu übernehmen. Die Anwendung schützt Prozesse, Treiber, Browser und die Hostdatei. Es handelt sich um eine Plattform für proaktiven Thread-Schutz für erfahrene Benutzer.

Leistungsstarke Echtzeitfunktionen: Diese Funktion lässt sich so konfigurieren, dass sie Versuche einzudringen protokolliert, meldet und blockiert.

Prozessschutz: Verhindert, dass schädliche Anwendungen die Kontrolle über andere Anwendungen übernehmen und weitere schädliche Inhalte auf Ihrem Computer installieren.

Treiberschutz: Verhindert das Installieren von Treibern und schützt vor anderen schädlichen Methoden, Low-Level-Zugriff auf Ihr Computersystem zu erlangen.

Schutz vor Browsermissbrauch: Überwacht die Einstellungen Ihres Internet Explorers und verwaltet Cookies. Außerdem ermöglicht dieses Tool das Protokollieren, Melden und Blockieren von Versuchen, Netzwerkfilter zu installieren, z. B. LSP (Layered Service Provider) und BHO (Browser Helper Object).

Schutz der Datei „HOSTS“: Schützt Ihre HOSTS-Datei vor unbefugter Manipulation. **Pharming-Schutz,** der durch den Schutz der HOSTS-Datei und die damit einhergehende Ausschaltung der meistverbreiteten Pharming-Angriffsmethode erfolgt.

Das Kunstwort **Pharming** ist aus den Begriffen „Phishing“ und „Farming“ zusammengesetzt (im nachstehenden Abschnitt „Spamschutz“ finden Sie eine Erläuterung des Begriffs „Phishing“). Von Pharming spricht man, wenn Sie beim Aufrufen einer Website durch Hackermanipulation auf eine andere, gefälschte Site umgeleitet werden. Pharming funktioniert so, dass entweder die Datei „HOST“ auf dem Zielcomputer verändert wird oder Schwachstellen in der DNS-Serversoftware ausgenutzt werden. Domänennamenserver (DNS) sind für die Auflösung von Internetnamen in die eigentlichen IP-Adressen zuständig. In den letzten Jahren wurden die Pharming- und Phishing-Methoden häufig zum Diebstahl von Online-Identitätsdaten eingesetzt. Pharming ist zu einem ernsten Problem für eCommerce-Unternehmen und im Onlinebanking geworden. Um dieser Bedrohung wirksam zu begegnen, sind komplexe Antipharming-Maßnahmen erforderlich.

Schutz vor dem Missbrauch von Prozessen (Process Hijacking Protection), der verhindert, dass bösartige Anwendungen einen „vertrauenswürdigen“ Prozess für das Einschleusen von DLL-Dateien oder Threads übernehmen

Startschutz (Launcher Protection), der Versuche einer Anwendung erkennt, sich selbst über eine andere Anwendung zu starten.

Installation

Das folgende Kapitel behandelt die Systemanforderungen, den Lizenzschlüssel, das Abrufen des Installationsprogramms und die Installation der Norman Security Suite auf Ihrem Computer.

Abrufen der Software

Beim Kauf der Norman Security Suite ist entweder eine CD mit Installationsprogramm im Lieferumfang enthalten, oder auf Ihrem Kaufbeleg ist ein Hyperlink für den Internetdownload vermerkt.

CD-ROM

Falls Sie eine CD-ROM von Norman erhalten haben, starten Sie damit die Installation.

Legen Sie die CD ins CD-ROM-Laufwerk ein.

Die CD startet automatisch, und das CD-Menü erscheint. Falls das CD-Menü nach ca. einer Minute noch nicht angezeigt wird, ist die AutoRun-Funktion möglicherweise deaktiviert. Um die CD manuell zu starten, gehen Sie folgendermaßen vor:

Durchsuchen Sie den Inhalt der CD, und klicken Sie auf die Root-Datei „Norman.exe“.

Klicken Sie nacheinander auf Start > Ausführen, und geben Sie „D:\Norman.exe“ ein, wobei Sie den tatsächlichen Laufwerksbuchstaben anstelle von „D“ setzen. Klicken Sie auf OK.

Wählen Sie die Sprache aus, in der das CD-Menü angezeigt werden soll.

Wählen Sie im CD-Menü auf der Seite Installieren die Sprache aus, die installiert werden soll.

Der InstallShield-Assistent wird gestartet. Gehen Sie zum Abschnitt „Installation läuft“ auf Seite <ÜS>.

Internetdownload

Das Installationsprogramm steht auch als Internetdownload zur Verfügung. Der Internetpfad und das Downloadverfahren sind in Ihren Kaufunterlagen beschrieben. Falls nicht, folgen Sie den nachstehenden Anweisungen, um das Installationsprogramm herunterzuladen und die Installation zu starten.

Öffnen Sie den Internetbrowser, und geben Sie die allgemeine Webadresse für Softwaredownloads von Norman ein: **http://www.norman.de/homedownloads**

Wählen Sie das entsprechende Installationsprogramm der Norman Security Suite für Ihre Sprache aus.

HINWEIS: Achten Sie auf die richtige Auswahl des Installationsprogramms für 64-Bit- bzw. 32-Bit-Computer.

Klicken Sie auf **Speichern** oder **Ausführen**.

Speichern

Falls Sie auf **Save** (Speichern) klicken, wird die Datei auf Ihrem Computer gespeichert und die Installation von dort gestartet. Für die Installation vom Computer aus ist keine Internetverbindung erforderlich. Allerdings empfehlen wir, die Internetverbindung auch während der Installation zur Schlüsselvalidierung und Aktualisierung aufrechtzuerhalten.

Suchen Sie einen Speicherort für das Installationsprogramm, und klicken Sie auf **Save** (Speichern), um den Vorgang zu bestätigen.

Notieren Sie sich den Speicherort des Installationsprogramms.

Damit sind Downloadfenster und Browser nicht länger erforderlich und können geschlossen werden.

Suchen Sie das Installationsprogramm, und öffnen Sie die Datei mit Doppelklick.

Nach erfolgter Installation kann das Installationsprogramm gelöscht werden. Eventuell sollten Sie eine Sicherungskopie erstellen.

Ausführen

Um die Installation direkt vom Internet aus zu starten, klicken Sie auf **Run** (Ausführen). Das Installationsprogramm wird daraufhin heruntergeladen und sofort gestartet. Sollte die Installation fehlschlagen, müssen Sie die Downloadseite erneut aufrufen.

Der InstallShield-Assistent wird gestartet. Gehen Sie zum Abschnitt „Installation läuft“ weiter unten.

Lizenzschlüssel

Mit dem Kauf der Norman Security Suite erhalten Sie einen Produktlizenzschlüssel. Dieser Schlüssel ist für die Aktualisierung des installierten Produkts erforderlich. Antivirenprogramme erfüllen nur dann ihren Zweck, wenn sie regelmäßig aktualisiert werden.
Ihr Installations Lizenzschlüssel hat das Format 5 x 5 Zeichen z.B. ABCDE-ABCDE-ABCDE-ABCDE-ABCDE

Ich besitze einen Schlüssel
Geben Sie den Schlüssel während der Installation nach Aufforderung durch den InstallShield-Assistenten ein. Dann sucht die Anwendung nach Abschluss der Installation automatisch nach Updates.

Ich besitze keinen Schlüssel
Sie können das Schlüsselfeld auch zunächst freilassen und trotzdem die gesamte Suite installieren.
Der Lizenzassistent fordert Sie dann jedoch in regelmäßigen Abständen zur Eingabe eines Schlüssels auf. Eine Aktualisierung des Produkts bzw. der Produkte erfolgt nicht.

Geben Sie nach Abschluss der Installation einen Schlüssel ein
Sie können den Lizenzassistenten der Anwendung starten und den Schlüssel in das vorgesehene Feld eintragen. Nähere Informationen finden Sie im Abschnitt „Lizenzassistent“ auf Seite <?>.

Installation läuft

Führen Sie den InstallShield-Assistenten der Norman Security Suite aus (das Installationsprogramm). Wie Sie diesen erhalten, erfahren Sie im Abschnitt „Abrufen der Software“ weiter oben in der Anleitung. Folgen Sie den Anweisungen auf dem Bildschirm. Um die Installationseinstellungen zu prüfen oder zu ändern, klicken Sie auf **Back** (Zurück).

Der Standardpfad für die Installation lautet C:\Programme\Norman**.**

Der Begrüßungsbildschirm des InstallShield-Assistenten erscheint. Klicken Sie auf **Next** (Weiter).

Lesen Sie die Lizenzvereinbarung, und akzeptieren Sie diese, um mit der Installation fortzufahren. Klicken Sie auf **Next** (Weiter).

Geben Sie einen gültigen Lizenzschlüssel ein. Klicken Sie auf **Next** (Weiter).

Der Schlüssel enthält Informationen zu den von Ihnen erworbenen Produkten.

Wenn Sie das Produkt nur testen möchten, können Sie dieses Feld freilassen. Wir empfehlen, einen Demoschlüssel einzugeben, um den vollen Funktionsumfang kennenzulernen.

TIPP

KOPIEREN SIE DEN LIZENZSCHLÜSSEL, UND FÜGEN SIE IHN EIN. Wenn ein Exemplar des Lizenzschlüssels in einer E-Mail oder in einem anderen elektronischen Format vorliegt, können Sie den Schlüssel einfach in das Feld für den Lizenzschlüssel kopieren. Dazu markieren Sie ihn und drücken dann **Strg+C**, um ihn zu kopieren. Anschließend setzen Sie den Cursor in das Feld für den Lizenzschlüssel und drücken **Strg+V**, um ihn einzufügen. Achten Sie darauf, dass der Lizenzschlüssel keine Leerzeichen enthält.

HINWEIS: Wenn Ihnen kein Lizenzschlüssel vorliegt, können Sie das Feld leer lassen und die Suite trotzdem vollständig installieren. Allerdings werden Sie vom Lizenzassistenten in regelmäßigen Abständen zur Eingabe eines Schlüssels aufgefordert. Eine Aktualisierung des Produkts bzw. der Produkte erfolgt nicht. Bei Bedarf hilft Ihnen der Lizenzassistent später beim Erwerb eines Schlüssels.

Das Dialogfeld „Setup Type“ (Setup-Methode)

Die Option **Complete** (Abschließen) sorgt für die Installation aller Programmfunktionen unter dem Standardpfad.

Wählen Sie **Complete** (Abschließen), und klicken Sie auf **Next** (Weiter).

Fahren Sie fort mit dem nachstehenden Punkt „7. Bereit zur Installation“.

Wählen Sie **Custom** (Benutzerdefiniert), um zu bestimmen, welche Produkte genau installiert werden sollen, und/oder um einen anderen Speicherpfad festzulegen.

Wählen Sie **Custom** (Benutzerdefiniert), und klicken Sie auf **Next** (Weiter).

Custom setup (Benutzerdefiniertes Setup)
Die installierbaren Produkte werden als Liste angezeigt.

Virenschutz

Bildschirmschoner Scanner

Spamschutz

Persönliche Firewall

Jugendschutz

Dieses Produkt müssen Sie manuell auswählen, falls es installiert werden soll. Klicken Sie auf das Dropdown-Menü linkerhand und anschließend auf die betreffende Funktion, um sie auf der lokalen Festplatte zu installieren. Die Installation dieses Produkts setzt voraus, dass es von Ihrem Lizenzschlüssel abgedeckt oder Teil Ihrer Testversion ist.

Sie können das Produkt nach Wunsch auch später installieren.

Datenschutzools

Eindringschutz

Klicken Sie auf **Space** (Speicherplatz), um zu sehen, wie viel Speicherplatz die ausgewählten Installationen erfordern.

Klicken Sie auf **OK**, um zum Dialogfeld **Custom setup** (Benutzerdefiniertes Setup) zurückzukehren.

Klicken Sie auf **Weiter**, um fortzufahren.

Zielordner

Klicken Sie auf **Next** (Weiter), wenn die ausgewählten Anwendungen unter dem Standardpfad gespeichert werden sollen.

Klicken Sie auf **Change...** (Ändern), um einen anderen Speicherort festzulegen.

Wählen Sie einen Speicherort aus der Dropdown-Liste, erstellen Sie einen neuen Ordner, oder geben Sie den Pfad im Eingabefeld für den Ordnernamen ein.

Klicken Sie auf **OK**, um zu bestätigen und zum Zielordner zurückzukehren.

Klicken Sie auf **Next** (Weiter).

Damit kann die Installation beginnen.

Klicken Sie auf **Install** (Installieren), um mit der Installation zu beginnen.

Installieren der Norman Security Suite.

Ein Dialog erscheint mit der Meldung, dass die Anwendung nun gestartet und die installierten Komponenten installiert werden können. Klicken Sie auf **OK**, um fortzufahren.

Ein Dialog meldet, dass der Vorgang abgeschlossen ist. Klicken Sie auf **Finish** (Fertigstellen), um den **InstallShield Wizard** (Assistenten) abzuschließen. Das Installationsprogramm wird noch weitere 5-10 Minuten im Hintergrund ausgeführt.

Klicken Sie auf **Restart now** (Jetzt neu starten), wenn Sie zum Neustart des Computers aufgefordert werden. Nach dem Neustart erscheint ein Kundenregistrierungsformular.

Kundeninformationen

Geben Sie bitte die erforderlichen Angaben ein, und klicken Sie anschließend auf **Submit** (Abschicken).

Installationsassistent

Nähere Informationen dazu finden Sie im nächsten Abschnitt.

Assistenten

Die Norman Security Suite verfügt über drei Assistenten. Sie sind für die Installation und Grundkonfiguration der Produkte zuständig.

InstallShield Wizard
Dieser Assistent dient zur Installation der Norman Security Suite. Er wird auch als Installationsprogramm oder Setup-Datei bezeichnet.

Installationsassistent
Dies ist bei der Installation der Personal Firewall von Bedeutung. Sobald die Norman Security Suite samt Personal Firewall installiert ist, wird ein Assistent für das Setup der Personal Firewall gestartet. Nähere Informationen dazu finden Sie im nächsten Abschnitt.

Lizenzassistent
Dieser Assistent verwaltet Ihre gültigen Produktlizenzen.

Installationsassistent

Nach erfolgter Installation der Norman Security Suite gehört die Persönliche Firewall nunmehr zu den installierten Funktionen. Die Firewall erkennt legitime und vertrauenswürdige Anwendungen automatisch und erzeugt automatisch Regeln für diese Anwendungen.

Sollten Sie zusätzliche Regeln hinzufügen wollen, gehen Sie wie folgt vor:

In der Security Suite 10.1 Oberfläche klicken Sie auf "Einstellungen" dann bei "Persönliche Firewall" auf das Stiftsymbol auf der rechten Seite.

Unter "Profi-Werkzeuge" starten Sie den Regelassistenten.

Erzeugen Sie nun eine Firewall Regel für die Anwendung, welche noch nicht in der Liste auftaucht bzw. welche Sie hinzufügen wollen.

Ggf. aktivieren Sie den erweiterten Regelassistenten wenn der normale Assistent nicht funktioniert oder Sie mit ihm nicht zurechtkommen, dieses machen Sie unter:

Unter "Erweiterte Einstellungen" - "Firewall-Operation" - "Erweiterten Regelassistenten verwenden".

Starten Sie nun den Regelassistenten und legen eine Regel für Ihre Anwendung an.

Testen Sie, ob Sie nun Ihre Anwendung normal nutzen können.

Erste Schritte

Anwendungssymbol in der Taskleiste

Während des Setups wird in der Taskleiste (am rechten unteren Bildschirmrand) ein Symbol platziert. Dieses Symbol bestätigt, dass die Norman Security Suite auf dem Computer installiert ist.



Mit einem Rechtsklick auf das Symbol rufen Sie das Taskleistenmenü der Security Suite auf.



Die Einträge sind folgende_

Internet Update: 

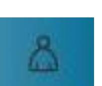
Aktivieren Sie die Funktion „Internet Update“, um die installierten Produkte zu aktualisieren.

Norman Security Suite Einstellungen: 

Öffnen Sie die Anwendung „Norman Security Suite“.

Computer prüfen: 

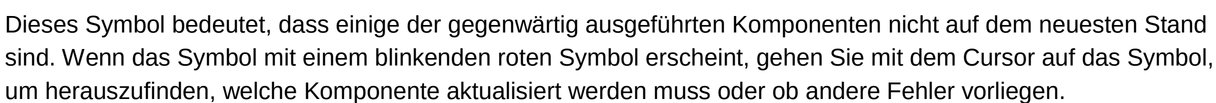
Hiermit starten Sie eine manuelle Prüfung des gesamten Computers.

Jugendschutz Benutzeranmeldung: 

Hier können Sie sich mit den Jugendschutzbenutzern anmelden. Dieser Punkt taucht nur auf, wenn die Komponenten Jugendschutz installiert ist.

Warnsymbole in der Taskleiste

Das Taskleistensymbol zeigt auch den Status der Security-Suite-Installation an. Gehen Sie mit dem Cursor über das Taskleistensymbol, um Erläuterungen zu Fehler- oder sonstigen Meldungen anzuzeigen.

Roter Kreis 
Dieses Symbol bedeutet, dass einige der gegenwärtig ausgeführten Komponenten nicht auf dem neuesten Stand sind. Wenn das Symbol mit einem blinkenden roten Symbol erscheint, gehen Sie mit dem Cursor auf das Symbol, um herauszufinden, welche Komponente aktualisiert werden muss oder ob andere Fehler vorliegen.

HINWEIS: Beim Systemstart wird das rote Symbol so lange angezeigt, bis alle Module gestartet wurden. Je älter und langsamer der Computer ist, desto länger dauert es, bis alle Module geladen wurden. Das normale Norman-Symbol sollte allerdings spätestens nach zwei Minuten erscheinen.

Gelbes Dreieck

Das gelbe Dreieckssymbol, das entweder statisch ist oder blinkt, zeigt an, dass der automatische Scanner manuell deaktiviert wurde, dass die Anwendung neu gestartet werden muss, dass ein Installationsfehler aufgetreten ist oder dass keine aktuellen Definitionsdateien vorliegen. Weitere Informationen erhalten Sie, wenn Sie mit dem Mauszeiger über dem Norman Symbol verweilen.

Statisch

Der automatische Scanner wurde manuell in den Einstellungen der Anwendung deaktiviert. Nähere Informationen finden Sie im Abschnitt „Automatischen Scanner aktivieren“.

Ein Neustart der Anwendung ist erforderlich. Bei einer zurückliegenden Aufforderung zum Neustart wurde möglicherweise die Option **Später neu starten** ausgewählt.

Es ist ein Installationsfehler aufgetreten. Versuchen Sie das Problem durch einen Neustart des Computers zu beheben.

Blinkend

Die Virendefinitionsdateien sind nicht mehr auf dem neuesten Stand. Das bedeutet, dass sie mindestens 5 Tage alt sind.

Der automatische Scanner wurde angehalten. Nähere Informationen finden Sie im Abschnitt „Automatischen Scanner aktivieren“.

Die Firewall wurde deaktiviert. Gehen Sie mit Rechtsklick auf das Taskleistenmenü und wählen Sie Einstellungen. Wählen Sie die Persönlichen Firewall Optionen aus (Stiftsymbol) klicken Sie auf den grünen Regler und wählen Sie aus „**Firewall aktivieren“**.

Gelbes Zahnrad

Wenn das angezeigte Taskleistensymbol ein Zahnrad trägt, greift der Norman Programm Manager (NPM) gerade auf das Programm zu, vermutlich zu Aktualisierungszwecken. Wir raten Ihnen, den Computer nicht auszuschalten, solange der NPM arbeitet, also solange dieses Symbol sichtbar ist.

HINWEIS: Ein Update sollte höchstens 5-10 Minuten dauern. Falls das Zahnradsymbol länger angezeigt wird, könnte ein Installationsproblem vorliegen. Versuchen Sie in diesem Fall, den Computer neu zu starten. Falls das Zahnrad auch nach erfolgtem Neustart noch angezeigt wird, wenden Sie die Reparaturoption an, die im Abschnitt „„Automatische Reparatur“ auf Seite <?> beschrieben ist.

Symbol des Windows Security Center

Norman ist ein Anbieter von Virenschutzprogrammen, die vom Betriebssystem erkannt werden. Wenn die Virendefinitionsdateien veraltet sind, der automatische Scanner inaktiv ist oder die Firewall deaktiviert wurde, erhalten Sie zudem eine Warnmeldung von Windows. Das Symbol des Security Center wird eingeblendet. Klicken Sie auf das Symbol, um die Windows-Einstellungen anzuzeigen und zu bearbeiten.

Öffnen der Anwendung

Sie können die Anwendung über das Taskleisten- oder das Windows-Menü aufrufen. Machen Sie mit der linken Maustaste, einen Doppelklick auf das Taskleistenmenü, es öffnet sich nun das Norman Security Suite Program Fenster. Alternativ klicken Sie im Windows-Menü auf **Start** und dann nacheinander auf **Alle Programme > Norman Security Suite > Norman Security Suite**.

Produktwarnsymbole

Gelegentlich erscheint ein gelbes Dreieck auf dem Menüeintrag der Anwendung. Das kann u. a. bedeuten, dass ein Produkt deaktiviert oder veraltet ist, die Lizenz abgelaufen ist oder eine neu installierte Software endgültig konfiguriert werden muss, um den Installationsvorgang abzuschließen.

HINWEIS: Wenn Sie die Security Suite zum ersten Mal öffnen, erscheint eine Warnmeldung bezüglich der Anwendung Jugendschutz. Nähere Informationen finden Sie im Abschnitt „Jugendschutz“.

Einstellungen der Security Suite

Diese Anwendung wird mit Standardeinstellungen installiert, und wir empfehlen, diese für den Alltagsbetrieb beizubehalten. Auf der Hauptseite der Anwendung können Sie die Option **Einstellungen** auswählen, um diverse Optionen für die Produkte zu konfigurieren.

Das Übersichtfenster sieht in etwa so aus:



Sie sehen eine Übersicht der einzelnen Module, welche Installiert sind.

Um die jeweiligen Standardeinstellungen zu ändern klicken Sie auf das Stiftsymbol: 

HINWEIS: Sie sollten die Standardeinstellungen nur ändern, wenn Ihnen klar ist, wie sich die Änderungen auf das System auswirken. Vergewissern Sie sich, dass die benutzerdefinierten Einstellungen die Sicherheitsstufe nicht herabsetzen. Falls Sie sich nicht sicher sind, sollten Sie bedenken, dass die Standardeinstellungen ausreichenden Schutz bieten.

Security Suite Startseite

Öffnen Sie die Anwendung „Security Suite“, um den Status der installierten Produkte anzeigen zu lassen. Näheres zum Öffnen der Anwendung erfahren Sie im Abschnitt „Erste Schritte“ weiter oben in dieser Anleitung.



Führen Sie eine Überprüfung des Computers durch (**Computer prüfen**), und ermitteln Sie, welche Produkte installiert sind, welchen Status sie haben und welche Detailinformationen zu ihnen vorliegen (**Letzte Ereignisse und Einstellungen**). Aktualisieren Sie alle Produkte (**auf Updates prüfen**), erstellen oder ändern Sie Scan Aufgaben (**Aufgaben**) oder schauen Sie ob auf Ihrem System, Viren o.ä. gefunden wurde (**Quarantäne**).

Um eine manuelle Prüfung des gesamten Computers zu starten, klicken Sie auf **Computer prüfen**. Anschließend können Sie zwischen verschiedenen Scan Arten wählen. Näheres zu diesen Punkten finden Sie im Kapitel über den manuellen Scanner.

Auf der linken Seite, sehen Sie, welche Version installiert ist und wir lange Ihre Lizenz gültig ist**.** Nähere Informationen finden Sie im Abschnitt „Lizenzschlüssel“.

Anhand des Statussymbols oben Rechts in im Fenster, erkennen Sie, ob die Installation auf dem aktuellen Stand und komplett ist, ob sie aktualisiert werden muss oder ob ein Produkt eventuell noch gar nicht installiert wurde.

HINWEIS: Wenn Sie die Security Suite zum ersten Mal öffnen, erscheint ggf. eine Warnmeldung bezüglich der Anwendung Jugendschutz. Nähere Informationen finden Sie im Abschnitt „Jugendschutz“.

Auf Updates prüfen

Aktualisieren Sie alle installierten Produkte mit einem einfachen Klick. Näheres zu weiteren Einstellungen sowie einen Überblick finden Sie im Abschnitt „Installieren und aktualisieren“.

Automatische Updates sind ein- bzw. ausgeschaltet.

Wenn die automatische Updatefunktion aktiviert ist, werden die Produkte regelmäßig aktualisiert.
Die Einstellungen können Sie unter „Aktualisierungsmethode auswählen“ auf Seite <?> bearbeiten.

HINWEIS: Es wird dringend empfohlen, die automatische Updatefunktion stets aktiviert zu belassen.

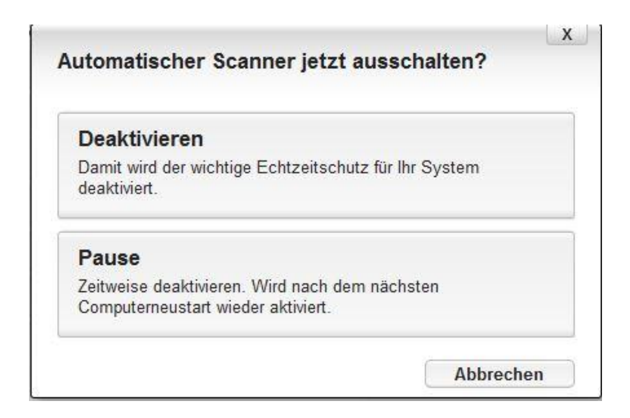
Virenschutz

Pausieren bzw. deaktivieren des Automatischen Scanners:

Im Hauptfenster der „Einstellungen“ der Norman Security Suite, klicken Sie auf den Schieberegler auf die Linke Seite:



Es öffnet sich anschließend ein Auswahlfenster:



Wählen Sie entsprechend aus, was Sie durchführen wollen.

Einstellungen Ändern

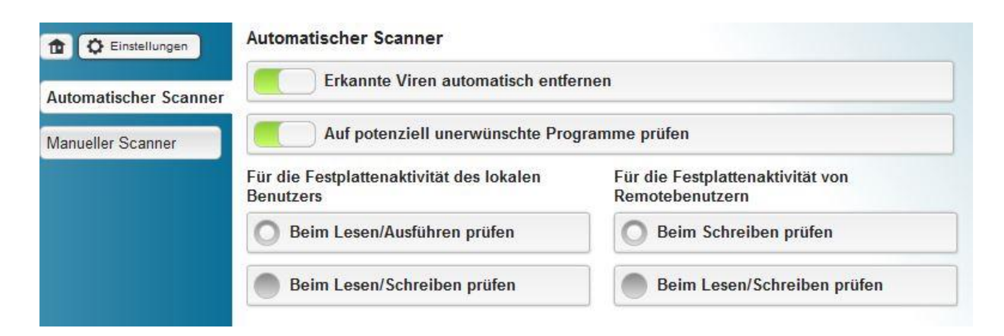
Öffnen Sie die Anwendung „Security Suite“, und wählen Sie den Punkt „**Einstellungen**“. Nähere Informationen zum Öffnen der Anwendung finden Sie im Abschnitt „Erste Schritte“ weiter oben in dieser Anleitung.

Anschließend klicken Sie auf das Konfigurationssymbol  um die Einstellungen für den „Virenschutz“ zu ändern.

Falls der Scanner manuell pausiert wurde, wird er beim nächsten Neustart des Computers oder bei der nächsten Installation eines Security Suite-Updates wieder aktiviert.

HINWEIS: Deaktivieren des Kontrollkästchens Automatischen Scanner bedeutet, dass der Scanner so lange deaktiviert wird, bis er manuell wieder eingeschaltet wird.

Hauptseite



Diese Virenschutz-Anwendung prüft Ihren PC auf schädliche Software, auch Malware genannt. Das vorliegende Kapitel behandelt die Konfiguration von zwei wichtigen Virenscannern, dem automatischen und dem manuellen Scanner.

Automatischer Scanner

Echtzeitprüfung von Dateien und Programmen bei Aufruf und Schreibzugriffen. Der automatische Scanner ist eine grundlegende Virenschutzkomponente, die permanent aktiv sein sollte.

Erkannte Viren automatisch entfernen

Der Scanner erkennt und repariert Viren aller Art. Wann immer dies möglich ist, wird eine infizierte Datei repariert und anschließend der Anwendung übergeben. Schlägt die Reparatur fehl, wird der Zugriff auf die infizierte Datei verweigert. Falls eine Datei ausschließlich Malware enthält, wird sie endgültig entfernt.

Benutzermodi

Der Abschnitt zu den Benutzermodi ist in die Module „Lokale Benutzer“ und „Dienste und Remotebenutzer“ eingeteilt. Unter normalen Umständen werden Workstations im Modus Lokale Benutzer und Server im Modus Dienst und Remotebenutzer ausgeführt. Die Standardeinstellungen bieten ausreichenden Schutz in den meisten Situationen, und wir empfehlen, sie nur dann zu ändern, wenn Ihnen die Folgen in vollem Umfang klar sind.

Lokaler Benutzer

Lesen/Ausführen

Hiermit wird der automatische Scanner angewiesen, Dateien zu prüfen, bevor sie geöffnet werden.

Beispiel: Wenn ein Benutzer mit Doppelklick eine DOC-Datei auswählt, überprüft der automatische Scanner nicht nur die Datei, sondern auch die entsprechende Anwendung, die geöffnet wird (in diesem Fall MS Word).

Beim Lesen und Schreiben prüfen

Hiermit wird der automatische Scanner angewiesen, Dateien zu prüfen, die zur Bearbeitung geöffnet werden und die beispielsweise aus dem Internet heruntergeladen wurden.

Bei Auswahl der Prüfoption **Lesen/Ausführen** kann es passieren, dass eine infizierte Datei auf die Festplatte heruntergeladen und gespeichert wird. Allerdings erkennt der automatische Scanner den Virus beim Öffnen der Datei.

Dienste und Remotebenutzer

Dieser Modus greift, wenn Computer mit den Betriebssystemen XP/Vista/Windows 7/8 abgemeldet werden und theoretisch als Server fungieren können. In diesem Abschnitt wählen Sie aus, ob Dateien geprüft werden sollen, bevor sie verwendet werden und/oder wenn neue Dateien erstellt oder vorhandene Dateien geändert werden. Mit anderen Worten, Sie wählen eine Strategie zur automatischen Prüfung aus, die zum Tragen kommt, wenn Sie aus dem Internet oder von FTP-Servern heruntergeladene Dateien speichern, wenn ein anderer Computer Dateien in eine Netzwerkfreigabe einstellt usw.

Schreiben

Hiermit wird der automatische Scanner angewiesen, Dateien zu prüfen, die auf der Festplatte gespeichert wurden, etwa wenn ein Benutzer eine Datei auf einem Server speichert. In diesem Fall prüft der automatische Scanner des betreffenden Servers die Datei.

Beim Lesen und Schreiben prüfen

Hierbei handelt es sich um eine Option, die Sie hoffentlich nicht in Anspruch nehmen müssen. Sie kann dann nützlich sein, wenn ein Server infiziert wurde, z. B. weil eine Scanneraktualisierung versäumt wurde. Eine Überprüfung sowohl beim Lesen als auch beim Schreiben sorgt dafür, dass sich der Befall nicht weiter im Netzwerk ausbreitet.

Sandbox

Die Sandbox-Funktion dient dazu, neue unbekannte Viren zu erkennen. Die Sandbox ist ein integraler Bestandteil der Norman Security Suite. Die Sandbox-Technologie ist speziell darauf abgestimmt, neue E-Mail-, Netzwerk- und Peer-to-Peer-Würmer sowie Dateiviren zu finden und auf unbekannte Gefahren für die Systemsicherheit zu reagieren.

Manueller Scanner

Mithilfe des manuellen Scanners können Sie ausgewählte Bereiche Ihres Computers prüfen. Die Überprüfung eines ganzen Laufwerks ist zeitaufwendig. Daher empfiehlt es sich, für die regelmäßige Überprüfung von bestimmten Laufwerken, Ordnern oder Dateien geplante Prüfungen einzurichten. Mithilfe des Aufgaben-Editors können Sie den Bildschirmschoner-Scanner so einrichten, dass manuelle Prüfungen automatisch in Zeiten von Leerlauf oder geringer Computerauslastung erfolgen. Schließlich können Sie den manuellen Scanner auch auf ein Objekt anwenden, indem Sie die entsprechende Option mit der rechten Maustaste auswählen. Die genannten Prüfverfahren verwenden sämtlich die Einstellungen des manuellen Scanners.

Sandbox

Die Sandbox-Funktion dient dazu, neue unbekannte Viren zu erkennen. Die Sandbox ist ein integraler Bestandteil der Norman Security Suite. Die Sandbox-Technologie ist speziell darauf abgestimmt, neue E-Mail-, Netzwerk- und Peer-to-Peer-Würmer sowie Dateiviren zu finden und auf unbekannte Gefahren für die Systemsicherheit zu reagieren.

Erkannte Viren automatisch entfernen

Hierbei versucht die Anwendung, den Virus aus einer infizierten Datei zu entfernen. Wählen Sie diese Option, um infizierte Dateien automatisch zu reparieren. Mit Ausnahme von Bootsektorviren lassen sich die meisten Viren direkt entfernen. Vor dem Entfernen eines Bootsektorvirus wird der Benutzer stets aufgefordert, den Vorgang zu bestätigen. Besteht eine Datei gänzlich aus Malware, wird die gesamte Datei gelöscht.

Archive prüfen

Wählen Sie diese Option, wenn Sie archivierte Dateien in den Scan aufnehmen möchten. Zurzeit werden die folgenden Formate unterstützt: ACE, APPLE_SINGLE, ARJ, BZIP2, CAB, GZ, LZH, MAIL, RAR, RAR3, SFXZIP, TAR, ZIP und 7Z.

Auf potenziell unerwünschte Programme prüfen

Ist diese Funktion ausgewählt wird auch Eine potentiell unerwüschte Software (Englisch PUP /potentially unwanted program) ist ein Programm welches ggf. unerwünschte Aktivitäten auf dem System durchführt

PUP kann z.B. Spyware, AdWare und oder Dialers beinhalten, welche häufig zusammen mit legitimer Software installiert wird.

Protokollierung

Protokolldatei erstellen

Hiermit wird bei jedem Ausführen eines manuellen Scans eine Protokolldatei im Ordner „C:\Programme\Norman\Logs“ erstellt. Wenn Sie diese Option deaktivieren, werden für manuelle Prüfungen keine Protokolldateien erstellt. Standardmäßig ist diese Option aktiviert.

Detaillierte Protokollierung

Bei der ausführlichen Protokollierung wird ein Bericht mit vielen Einzelheiten erstellt, in dem jede durchsuchte Datei, Prüfdauer pro Datei, Status usw. angegeben ist.

Weitere Prüfverfahren

Kontextmenü-Scanner
Hierbei handelt es sich um einen manuellen Scanner, mit dem Sie aktuell markierte Dateien oder Ordner prüfen lassen können, indem Sie mit der rechten Maustaste das Windows-Kontextmenü aufrufen.

Klicken Sie dazu mit der rechten Maustaste auf eine Datei oder einen Ordner und Sie sehen im Kontextmenü den Punkt:

 Prüfung auf Viren

Dies funktioniert beispielsweise im Windows Explorer oder auf dem Desktop.

Wählen Sie aus dem Popup-Menü die Option **Prüfung auf Viren**.

Das Dialogfeld **Manueller Scanner** wird angezeigt. Sie können den Computer nach weiteren Dateien oder Ordnern **Durchsuchen**, die geprüft werden sollen, und den Prüfvorgang mithilfe der Optionen **Start**, **Pause** oder **Stop** entsprechend steuern.

Befehlszeilen-Scanner

Sie können statt des Scanners mit Benutzeroberfläche auch die Befehlszeilenprüfung einsetzen, etwa um Stapelaufträge und andere Prüfaufgaben über die Befehlszeile auszuführen. Die Befehlszeilenprüfung ist eine gute Alternative für Benutzer, die mit dieser Umgebung vertraut sind.

Der Befehlszeilen-Scanner hat dieselben Basisfunktionen wie die menügesteuerten Scanner und hängt nicht von anderen Modulen ab. Er kann auch über Stapeldateien ausgeführt werden.

Starten des Befehlszeilen-Scanners

Rufen Sie die Eingabeaufforderung auf.

Wählen Sie Start **>** Ausführen**.**

Geben Sie „CMD“ ein, und klicken Sie auf OK**, oder drücken Sie die** Eingabetaste**.**

Gehen Sie in das Verzeichnis, in der die Anwendung „Antivirus“ zu finden ist.
Der Standardpfad lautet C:\Programme\Norman\nvc\bin\.

Geben Sie die gewünschten Parameter ein, und drücken Sie die Eingabetaste.

Um eine Liste der verfügbaren Parameter aufzurufen, geben Sie folgenden Befehl ein:

nvcc /?

Die Syntax hierfür lautet:

nvcc [Laufwerk]:[Pfad] [/Parameter] [Eingabetaste]

Vor jedem Parameter, den Sie verwenden, muss ein Leerzeichen stehen.

Quarantäne



Die Quarantäne in der Security Suite können Sie über die Hauptseite über den Punkt „Quarantäne“ aufrufen.

Dateien / Elemente in Quarantäne

Infizierte Dateien in Quarantäne sind in einer Liste im Dialogfeld **Quarantäne** aufgeführt, sofern Sie das Programm so konfiguriert haben. Das Antivirenprogramm versucht, infizierte Dateien vor dem Löschen und/oder der Überführung in die Quarantäne (je nach Konfiguration) zu reparieren. Dateien in Quarantäne sind entweder infiziert oder es handelt sich um potentiell Unerwünschte Software / Programme..

!!! HINWEIS: Eine Kopie der gelöschten oder blockierten Datei wird standardmäßig in Quarantäne genommen.

Eine Kopie der infizierten und unter Quarantäne gestellten Datei wird gelöscht, es sei denn, sie befindet sich in einem anderen Ordner. In diesem Fall wird sie in Quarantäne verschoben. Wenn der automatische Scanner erkennt, dass z.B. C:\eicar.com infiziert ist, wird die Datei in Quarantäne genommen. Wenn allerdings der automatische Scanner C:\Kopie von eicar.com entdeckt und feststellt, dass diese identisch mit eicar.com ist, wird sie nicht in Quarantäne genommen, sondern gelöscht. Wenn C:\Kopie von eicar.com sich in C:\anderer Ordner\ befindet, wird die Datei jedoch aufgrund des neuen Speicherorts in Quarantäne genommen. Dieses Verfahren soll verhindern, dass die Quarantäne überfüllt wird, wenn ein Virus mehrere Kopien derselben Datei in denselben Bereich des Laufwerks geschrieben hat.

Dateien können auch unter Quarantäne gestellt werden, wenn die Antivirenanwendung vermutet, dass sie infiziert sind. In seltenen Fällen kann es auch nach der Aktualisierung der Definitionsdateien vorkommen, dass die Antivirenanwendung feststellt, dass zuvor unter Quarantäne gestellte Dateien doch harmlos sind (False Positive). Da Typen und Methoden zum Herstellen und Erkennen von Viren sich rasant weiterentwickeln, prüfen Antivirenprogramme die Quarantänedateien nach jedem Update und nach jedem Neustart des Computers.

Falls eine solche Prüfung die Harmlosigkeit einer in Quarantäne befindlichen Datei feststellt, wird diese wiederhergestellt, sofern ein gültiger Dateipfad vorliegt und keine weitere Datei gleichen Namens existiert. Dazu ist kein Benutzereingriff erforderlich, und die mögliche Wiederherstellung einer unter Quarantäne gestellten Datei wird dem Benutzer auch nicht gemeldet.

Aufgaben-Editor

Manchmal ist es von Nutzen, Scan Aufgaben festzulegen, die mehrmals und/oder in regelmäßigen Abständen ausgeführt werden müssen. Das Überprüfen auf Viren ist ein gutes Beispiel für eine Aufgabe, die regelmäßig ausgeführt werden muss, und der Aufgaben-Editor ist das entsprechende Werkzeug dafür.

Sie können eine Aufgabendatei für Scans erstellen, die wiederholt durchgeführt werden sollen, oder für besondere Scans, die in bestimmten Situationen durchgeführt werden sollen. Wenn Sie beispielsweise Dateien aus dem Internet in dafür vorgesehene Bereiche herunterladen, können Sie eine Aufgabendatei erstellen, die nur diese Bereiche prüft, und die Aufgabe nach dem Herunterladen manuell ausführen. Außerdem können Sie einen Zeitplan für den Task erstellen, damit er zu einer festgelegten Zeit durchgeführt wird z.B. einmal wöchentlich.

HINWEIS: Das Dialogfeld Eine Aufgabe erstellen erscheint beim ersten Aufrufen des Aufgaben-Editors oder falls noch keine Aufgaben erstellt wurden.

Alle bestehenden Aufgaben werden unter dem Punkt Aufgaben angezeigt:



Abhängig davon, welche Security Suite Version Sie im Einsatz bzw. lizenziert haben, haben Sie bereits vorgefertigte Aufgaben, welche Sie aktivieren und über den Button  nachträglich bearbeiten können.

Programmverlauf löschen

Unter diesem Punkt können Sie auswählen, ob Programmverläufe automatisch gelöscht werden sollen. Dieses können Sowohl Windows eigene Verläufe sein als auch Internet Browser Verläufe. Details sehen Sie, wenn Sie auf den Bearbeiten Button  klicken. Programmverläufe löschen ist ein Bestandteil der Datenschutztools.

Bildschirmschoner-Scanner

Wenn Sie den Bildschirmschoner-Scanner aktivieren, wird Ihr System bei Leerlauf auf Viren geprüft. Die Dauer der Nichtbenutzung ist als der Zeitraum definiert, in dem das System keine Aktivitäten verzeichnet, d. h. Eingaben weder über die Tastatur noch über die Maus erfolgen.

Beim Start des Bildschirmschoners startet der manuelle Scanner eine Prüfung aller Festplatten. Sobald der Computer etwa durch eine Mausbewegung oder Tasteneingabe wieder in Betrieb genommen wird, hält die Bildschirmschoner-Prüfung an. Falls die Prüfung zu diesem Zeitpunkt noch nicht abgeschlossen sein sollte, wird sie bei der nächsten Leerlaufphase an dem Punkt, wo sie unterbrochen wurde, fortgesetzt.

Wenn Sie den Bildschirmschoner aktivieren, wird dieser nach der Konfigurierten Leerlaufphase bzw. Timer gestartet. Wenn Sie dieses ändern wollen, klicken Sie auf den Bearbeiten Button 

Sobald der Norman-Screensaver durch die nächste Leerlaufphase aktiviert wird, beginnt der manuelle Scanner mit der Prüfung der Festplatten, wobei der Prüfungsfortschritt ständig angezeigt wird. Den Bildschirmschoner-Scanner beenden Sie durch Betätigen einer beliebigen Taste oder durch Bewegen der Maus.

HINWEIS: Die Bildschirmschoner-Prüfung verwendet die gleichen Einstellungen wie die des manuellen Scanners.

Systemprüfung

Wenn diese Option aktiviert ist, überwacht die Systemprüfung Ihr System auf bösartiges Verhalten und verdächtige Hintergrundpgrogramme und sperrt verdächtiges Verhalten.

Geplanter Virenscan

Wenn diese Option aktiviert ist, wird zum konfigurierten Zeitpunkt ein schneller Scan „Quick_Scan“ durchgeführt. Beim Quick_Scan wird das c:\programme, c:\windows und der komplette Arbeitsspeicher durchgescannt.

Aufgabe Hinzufügen

Wählen Sie diesen Punkt aus, um neue Scan bzw. Prüfaufgaben hinzuzufügen, wenn Sie z.B. einen Vollständigen Systemscan oder einen Benutzerdefinierten Scan hinzufügen wollen. Anschließend können Sie noch das Intervall definieren z.B. täglich, wöchentlich etc.

Ausschlussliste

Im Einstellungen Menü finden Sie den Punkt „Ausschlussliste“:



In der Ausschlussliste enthaltene Dateien werden nicht geprüft. Dateien können beispielsweise vom Prüfvorgang ausgeschlossen werden, wenn sie Fehlalarme auslösen oder die Prüfung zu zeitaufwendig ist. Es wird aber empfohlen, Dateien in der Ausschlussliste in regelmäßigen Abständen durch geplante oder manuelle Scans zu prüfen.

> **HINWEIS: Ausschlusslisten sollten äußerst sorgfältig verwaltet werden, da sie ein potenzielles Sicherheitsrisiko darstellen. Das Ausschließen von Dateien oder Bereichen von der Überprüfung geht auf Kosten der Sicherheit.**

Ausschlussliste verwenden

Wenn Sie den grünen Schieberegler auf die linke Seite schieben bzw. klicken, können Sie diese Option deaktivieren. Die **Ausschlussliste** dient zum Ausschließen von Dateien, bei denen ein Konflikt mit den Scannern besteht, der sich auf die Leistung des Computers auswirkt.

Dateien von der Überprüfung ausschließen

Um die Ausschlussliste zu konfigurieren, klicken Sie auf das Konfigurationssymbol: 

Legen Sie Dateien, Verzeichnisse oder ganze Laufwerke fest, die nicht auf Malware überprüft werden sollen. Führen Sie die folgenden Schritte durch, um Elemente vom Scanvorgang auszuschließen:

Klicken Sie auf das Ordner Symbol für die Ordnersuche, um nach Dateien und Ordnern zu suchen, oder geben Sie einen Dateinamen, Verzeichnis oder Laufwerksbuchstaben in das Eingabefeld ein und klicken Sie auf „Hinzufügen“:



Platzhalterzeichen (*/?) werden unterstützt. Setzen Sie den Platzhalter am Anfang oder am Ende des Suchbegriffs. Setzen Sie den Platzhalter nicht in der Mitte des Suchbegriffs.

HINWEIS: Verwenden Sie bei der Angabe auszuschließender Elemente KEINE Anführungszeichen („oder“).

Beispiele

C:\Dir	Schließt alle im angegebenen Verzeichnis und den Unterverzeichnissen enthaltenen Dateien aus.
*.xyz	Schließt alle Dateien mit der Dateierweiterung „.xyz“ aus.
example.exe	Schließt die angegebene Datei ungeachtet des Speicherorts aus.
C:\System\xyz.doc	Schließt diese spezielle Datei aus.
C:\dir*.log	Schließt im angegeben Verzeichnis alle Dateien mit der Endung .log aus

Bestimmen Sie, welchen Scanner die Ausschlussliste ggf. verwenden sollte.

Um einen Eintrag der Ausschlussliste hinzuzufügen, klicken Sie auf **Hinzufügen**.

HINWEIS: Die Security Suite prüft nicht, ob es die Dateien, Ordner oder Laufwerke, die Sie der Ausschlussliste hinzufügen, tatsächlich gibt. Deshalb dürfen Sie bei der Eingabe von Namen und Pfaden keine Fehler machen.

Netzwerklaufwerke

Sie können auch Netzwerklaufwerke wenn keine Freigaben auf entfernten Computern, auf die Sie Zugriff haben, geprüft werden sollen. Geben Sie ggf. auch den betreffenden Scanner an.

Auswahl löschen

Wenn Sie Einträge aus der Ausschlussliste entfernen möchten, wählen Sie den gewünschten Eintrag und klicken auf das Papierkorbsymbol um den Eintrag zu entfernen.

HINWEIS: Es ist ratsam, die Ausschlussliste in regelmäßigen Abständen zu überarbeiten.

Persönliche Firewall

Öffnen Sie die Anwendung „Security Suite“, und wechseln Sie zunächst auf den Punkt „Einstellungen“. Dort finden Sie die Option **Persönliche Firewall**. Nähere Informationen zum Öffnen der Anwendung finden Sie im Abschnitt „Erste Schritte“.

Hauptseite

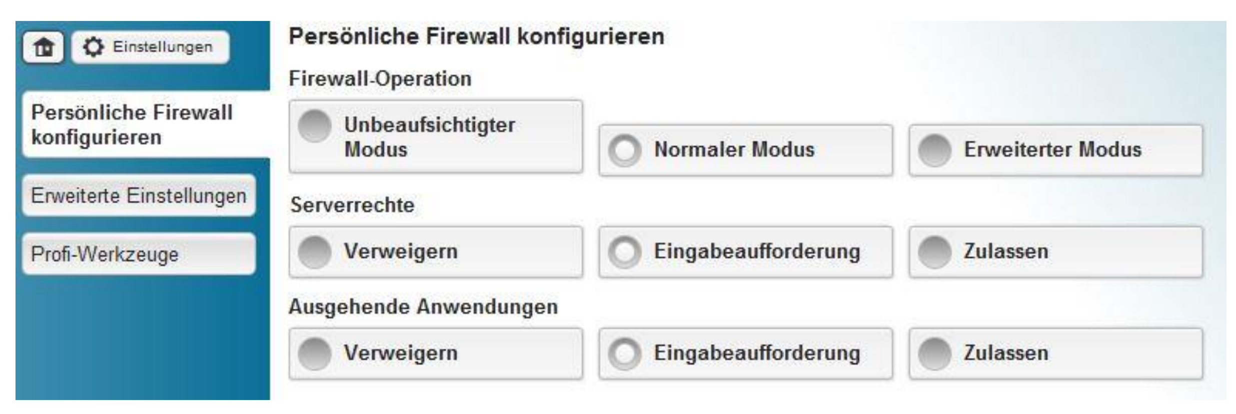
Dieses Kapitel behandelt die Konfiguration der Firewall-Anwendung, das Erstellen der Regeln für ein- und ausgehende Anwendungen, das Anzeigen des Datenverkehrs und weitere Themen. Die Anwendung unterscheidet zwischen erfahrenen und unerfahrenen Benutzern. Während der unerfahrene Benutzer vom Installationsassistenten geführt wird, haben erfahrene Benutzer die Möglichkeit, die erweiterten Einstellungen bis ins Detail zu konfigurieren.

Einstellungen anpassen

Klicken Sie auf den Konfigurationsbutton  um die Standardwerte zu bearbeiten.

Persönliche Firewall konfigurieren

Die Konfigurationsseite ist in drei Punkte gegliedert:



Es können die Firewall Operationen ausgewählt werden und Sie können pauschal definieren wie mit Firewall Vorfällen gehandhabt wird. Standardmäßig wird der Benutzer durch eine „Eingabeaufforderung“ gefragt.

Nachstehend ist die Option „Personal Firewall-Operation“ beschrieben.

Unbeaufsichtigter Modus: Die persönliche Firewall lässt allen Datenverkehr zu, der nicht durch eine spezielle Regel blockiert wird. Sie ist im Hintergrund unbemerkt aktiv und schützt ohne jegliche Benutzereingriffe gegen Angriff von außen.

Normaler Modus: Dieser Modus ist per default ausgewählt. Bei unbekannten Datenverkehr wird sofort eine Eingabeaufforderung eingeblendet. Es wird ein Popup mit Details zu der Anwendung angezeigt, die den Netzwerkzugriff versucht. Mithilfe von permanenten oder nur für die aktuelle Sitzung gültigen Regeln können Sie festlegen, ob der Verkehr zugelassen oder verweigert werden soll. Somit sind Sie sowohl gegen Angriffe von außen als auch gegen das unerwünschte Versenden Ihrer Daten durch Anwendungen auf dem Computer geschützt.

Erweiterter Modus: Diese Firewall-Operation entspricht im Wesentlichen dem normalen Modus, allerdings wird die DPI-Funktion (Deep Process Inspection) standardmäßig aktiviert. Die DPI-Funktion bietet erweiterten Schutz gegen Trojanerangriffe, bei denen versucht wird, Daten durch die Firewall zu schmuggeln. Die Protokollierung ist detaillierter und umfasst eine vollständige Aufstellung aller Dienste, die im Kontext einer SVchost.exe- Sitzung ausgeführt werden. Da die DPI-Funktion viele Ressourcen in Anspruch nimmt, wird sie aus Leistungsgründen für langsamere Computer nicht empfohlen. Aufgrund dieser Leistungseinbußen kann es möglicherweise auch zu Kompatibilititäsproblemen mit Anwendung von Drittanbietern kommen. Das liegt daran, dass der Paketempfang einige Millisekunden länger dauern kann, sodass in einigen Fällen das erste an die Anwendung gesendete Paket verlorengeht (und erneut gesendet werden muss). Wenn bei einer Ihrer Anwendungen solche Probleme auftreten, können Sie die DPI-Funktion über eine Regel im erweiterten Regelassistenten deaktivieren

Serverrechte
Manche Anwendungen ohne Regeln versuchen eventuell, Verbindungen aus dem Internet zuzulassen. In diesem Dialogfeld können Sie bestimmen, wie die Personal Firewall mit solchen Anwendungen verfahren soll. Die Standardeinstellung lautet **Eingabeaufforderung**. Nach Aufforderung können Sie selbst einschätzen, ob die betreffende Anwendung Netzwerkeinladungen annehmen darf. Alternativ können Sie **Verweigern** festlegen, sodass sämtliche Programme ohne permanente oder sitzungsbasierte Regel Netzwerkeinladungen ablehnen.

Ausgehende Anwendungen
Unter Umständen greifen auch Anwendungen, für die keine Regeln vorliegen, auf das Internet oder das LAN zu. In diesem Dialogfeld können Sie bestimmen, wie die Personal Firewall mit solchen Anwendungen verfahren soll. Die Standardeinstellung lautet **Eingabeaufforderung**. Nach Aufforderung können Sie beispielsweise die betreffende Anwendung selbst einstufen und eine Regel festlegen. Alternativ können Sie **Verweigern** festlegen, sodass sämtlichen Programmen ohne permanente oder sitzungsbasierte Regel der Netzwerkzugriff verweigert wird.

Erweiterte Einstellungen

Der technische Charakter dieser Konfigurationsoptionen erfordert ein gewisses Fachwissen, um die Standardeinstellungen zu ändern. Als Faustregel gilt, dass Sie Einstellungen nur dann ändern sollten, wenn Ihnen deren Bedeutung und die Folgen der Änderung bekannt sind. Für den Durchschnittsbenutzer sind die Standardeinstellungen ausreichend. Erfahrene Benutzer können jedoch weitere Einstellungen der Firewall vornehmen, wie z.B. mit bestimmten Netzwerkressourcen oder Windows Funktionen verfahren werden soll.

Profi-Werkzeuge

Regelassistent

Regeln werden benötigt, um „vertrauenswürdigen“ Anwendungen den Zugriff auf das Internet zu ermöglichen. Darauf sind viele moderne Programme angewiesen.

Im Zuge der Installation wurden automatisch mehrere Regeln erstellt, darunter solche für gängige Browser, Mail-Clients, MSN und weitere Programme, die auf das Internet zugreifen müssen.

(Sollte dieses bei Ihnen einmal nicht funktioniert haben oder Sie den manuellen Wizard durchlaufen wollen, wechseln Sie in das Verzeichnis *c:\programme\norman\npf\bin* und starten Sie den Wizard per *npfwiz.exe.)*

Es können jedoch auch Programme installiert sein, die von der Firewall nicht erkannt werden oder erst nach der Installation der Firewall hinzugekommen sind. Wenn ein solches Programm versucht, eine Verbindung zum Internet herzustellen, öffnet die Personal Firewall ein Popup-Fenster, in dem Sie über diesen Vorgang informiert werden und entscheiden können, ob der Zugriff zugelassen oder verweigert werden soll.

Regeln für eingehende Verbindungen können Sie mit der Personal Firewall nicht erstellen. Diese werden auf der Basis der Entscheidungen im Servermodus der Personal Firewall angelegt. Dies erfolgt dynamisch und automatisch sowie auf Grundlage von Serverrechten. Dabei handelt es sich um einen intelligenten Mechanismus der Firewall, der Zugriffsversuche von außen auf eine Gruppe von Ports auswertet. Legitimen Anforderungen wird der Zugriff für die relevanten Ports gewährt. Wenn dies nicht mehr erforderlich ist, werden die Ports automatisch geschlossen.

Regel anlegen

In der Security Suite 10 Oberfläche klicken Sie auf "Einstellungen" dann bei "Persönliche Firewall" auf das Stiftsymbol auf der rechten Seite.

Unter "Profi-Werkzeuge" starten Sie den Regelassistenten.

Erzeugen Sie nun eine Firewall Regel für die Anwendung, welche die Verbindung nicht aufbaut.

Ggf. aktivieren Sie den erweiterten Regelassistenten wenn der normale Assistent nicht funktioniert, dieses machen Sie unter:

"Erweiterte Einstellungen" - "Firewall-Operation" - "Erweiterten Regelassistenten verwenden".

Starten Sie nun den Regelassistenten und legen eine Regel für Ihre Anwendung an.

Testen Sie, ob Sie nun Ihre Anwendung normal nutzen können.

Dienstprogramm für Echtzeitprotokoll

Die Personal Firewall nutzt ausgefeilte Tarntechniken, um Ihren Computer gegenüber dem Internet abzuschirmen und zu verbergen. Mit zwei weiteren Funktionen können Sie die Aktivitäten auf Ihrem Computer überwachen: **Dienstprogramm für Echtzeitprotokoll** und **Erweiterte Port-Anzeige**.

Unter Profi-Werkzeuge klicken Sie auf **Dienstprogramm für Echtzeitprotokoll**. Klicken Sie mit der rechten Maustaste auf einen Eintrag, um Details anzuzeigen und ggf. die Konfiguration für die betreffende Anwendung zu ändern.

Ausgehender Datenverkehr
Das Protokoll hält Folgendes fest: zu welcher **Zeit** eine **Anwendung** auf das Internet zugegriffen hat, den Programmnamen und den benutzten **Port**. Ferner vermerkt es die IP-Adresse, den Port des **Remote-Computers** und die jeweilige **Aktion**. Die **Aktion** wird entweder zugelassen oder verweigert. Die **Ursache** ist entweder, dass eine permanente Regel oder eine Sitzungsregel für die betreffende Aktion bzw. Anwendung vorliegt, sofern sie in der **Erweiterten Konfiguration** definiert ist, oder eine Zeitüberschreitung bei der Benutzeraufforderung.

Anforderungen von Serverrechten
Das Protokoll hält Folgendes fest: zu welcher **Zeit** eine **Anwendung** auf den Computer vom Internet aus zugegriffen hat und den benutzten **Port**. Ferner vermerkt es die IP-Adresse, den Port des **Remote-Computers** und die jeweils von der Personal Firewall ergriffene **Aktion**. Die **Aktion** wird entweder zugelassen oder verweigert. Die **Ursache** ist entweder, dass eine permanente Regel oder eine Sitzungsregel für die betreffende Aktion bzw. Anwendung vorliegt, die in der **Erweiterten Konfiguration** definiert ist, oder dass keine empfangende Anwendung vorhanden ist. Der häufigste Grund für die Ablehnung von Anforderungen von Serverrechten ist, dass Ihr Computer nicht über die erforderliche Software zur Interpretation der Anfrage verfügt. Mit anderen Worten, es liegen keine Serverrechte vor, die der Anforderung entsprechen.

Um Daten von einem anderen Computer im Netzwerk zu empfangen, öffnet eine Anwendung mindestens einen empfangsbereiten Port. Hierbei ist zu beachten, dass Anforderungen von Serverrechten keine eingerichteten Verbindungen darstellen, sondern nur Anforderungen von Verbindungen. Allerdings öffnet eine Anwendung manchmal auch einen empfangsbereiten Port, um die Antwort eines Computer zu empfangen, an den sie Daten versendet hat. Die Personal Firewall lässt solche Antworten automatisch zu. Ein Mechanismus der Personal Firewall ermittelt, ob eine Anwendung einen Port absichtlich geöffnet hat oder ob die Anwendung eine unerwünschte Anfrage erhält, als handele es sich um einen Server. Daraufhin fordert die Personal Firewall den Benutzer auf zu bestätigen, dass die Anwendung Serverrechte erhalten soll.

Erweiterte Port-Anzeige

Die erweiterte Port-Anzeige bietet eine Übersicht aller Aktivitäten an den Ports des aktuellen Computers. Dieses Dienstprogramm dient zur manuellen Prüfung, ob Ihr Computer von Malware befallen ist.

Unter Profi-Werkzeuge klicken Sie auf **Erweiterte Port-Anzeige**.

Ports, die für das Internet geöffnet sind, werden rot angezeigt und erfordern Ihre volle Aufmerksamkeit, denn die Firewall kann einen offenen Port nicht schützen. Die Nutzung offener Ports durch Serversoftware wie FTP- und Webserver ist zulässig. Wenn allerdings eine unbekannte Anwendung einen offenen Port aktiv nutzt, besteht Anlass zur Sorge.

Anwendung anhalten

Um eine Anwendung anzuhalten, markieren Sie einen Eintrag und klicken auf **Anwendung beenden**. Die Anwendung wird sofort beendet, selbst wenn sie noch etwa eine Minute lang in der Liste angezeigt wird.

Eingabe der Option „Erweiterte Konfiguration öffnen“

Markieren Sie einen Eintrag, und wählen Sie die Option **Erweiterte Konfiguration öffnen**.

> **HINWEIS: Wenn Sie für die Konfiguration einer Anwendung „Verweigern“ statt „Zulassen“ festlegen möchten, entfernen Sie das Häkchen. Klicken Sie dann auf OK. Wenn einer Anwendung der Zugriff auf das Internet doch gewährt werden soll, setzen Sie ein Häkchen. Beachten Sie, dass „Anwendung beenden“ und „Zugeordnete Regel bearbeiten“ nur für Einträge gilt, für die eine Regel erstellt wurde. Die Option „Erweiterte Konfiguration öffnen“ ist nur für Regeln verfügbar, die unter die „erweiterte Konfiguration“ fallen.**

Einstellungen

Personal Firewall konfigurieren

Personal Firewall deaktivieren / aktivieren oder deinstallieren

Im Hauptfenster der „Einstellungen" der Norman Security Suite, klicken Sie auf den Schieberegler auf die Linke Seite bei „Persönliche Firewall":



Es öffnet sich anschließend ein Auswahlfenster:



Wählen Sie entsprechend aus, was Sie durchführen wollen.

Durch Anklicken des Deaktivieren Buttons wechseln Sie zwischen aktiviertem und deaktiviertem Status der Persönlichen Firewall.

HINWEIS: Das Windows Security Center gibt bei Deaktivierung der Firewall eine Warnmeldung aus.

Wenn Sie die Firewall deinstallieren, wird die Komponente Deinstalliert und Ihre Norman Installation bittet Sie anschließend ggf. das System neu zu starten um den Vorgang abzuschließen**.**

Spamschutz

Öffnen Sie die Anwendung „Security Suite“, und wählen Sie unter „Einstellungen“ die Option **„Spamschutz“** aus. Nähere Informationen zum Öffnen der Anwendung finden Sie im Abschnitt „Erste Schritte“ in dieser Anleitung.

Hauptseite

Diese Anwendung schützt vor unerwünschten Werbe- und Massensendungen per E-Mail (sogenanntem „Spam“), die u. U. eine Bedrohung für das System darstellen. In diesem Kapitel erfahren Sie, wie Sie Spamfilter anpassen, Sperr- und Zulassungslisten erstellen, gefilterte E-Mails verwalten und einsehen und Updateintervalle festlegen. Ferner werden Spamverwaltungsoptionen behandelt.

Spamstatistik

Die grafische Ansicht zeigt an, wie viele Spam-Mails und Phishing-Angriffe von der Anwendung in den letzten beiden Wochen pro Tag blockiert wurden.

Einstellungen anpassen

Klicken Sie auf diese Option, um die Standardwerte zu bearbeiten.

Sperren/Zulassen

Mithilfe der Sperr-/Zulassungsliste können Sie einzelne E-Mail-Adressen verwalten, um für die Anwendung festzulegen, welche Adressen immer zugelassen bzw. immer abgelehnt werden sollten. Die Antispam-Filtermethode setzt nie Ihre manuellen Anweisungen bezüglich einer Adresse außer Kraft (Sperren bzw. Zulassen).

Gefilterte E-Mail-Nachrichten anzeigen

Hiermit können Sie sich anzeigen lassen, welche E-Mail-Nachrichten beispielsweise aus Microsoft Outlook, Outlook Express oder Windows Mail ausgefiltert wurden. Der NAS-Spamfilter wird im Zuge der Installation der Norman Security Suite erstellt oder wenn Sie einen der vorgenannten E-Mail-Clients installieren und Norman Security Suite auf Ihrem Computer bereits ausgeführt wird.

Öffnen Sie Ihren meistbenutzten E-Mail-Client, und suchen Sie nach dem NAS-Spamfilter und dem Antispam-Anwendungsmenü.

Spam melden

Hiermit werden bestimmte E-Mails als Spam gemeldet. Wählen Sie eine E-Mail-Nachricht im Eingangsordner, und klicken Sie in der Symbolleiste auf die Option **Spam melden**. Die Nachricht wird in den Ordner **NAS Spam** verschoben.

Kein Spam

Hiermit werden verdächtige E-Mails als zulässig gekennzeichnet. Markieren Sie mindestens eine E-Mail im Ordner **NAS Spam**, und klicken Sie auf **Kein Spam**.

Sperren/Zulassen

Hiermit können Sie E-Mail-Adressen sperren oder zulassen Die Auswahl dieser Option öffnet die Anwendung „Norman Antispam“. Geben Sie mindestens eine E-Mail-Adresse ein, und wählen Sie entweder **Sperren** oder **Zulassen**.

Spam entfernen

Hiermit löschen Sie den gesamten Inhalt der Ordners NAS Spam. Um E-Mails einzeln zu löschen, klicken Sie den betreffenden Eintrag mit der rechten Maustaste an, und wählen Sie im Kontextmenü die Option Löschen.

Ordner überprüfen

Hiermit prüfen Sie den E-Mail-Eingang auf Spam. Wählen Sie mindestens einen Ordner aus, und klicken Sie auf die Option „Ordner prüfen“, um eine manuelle Prüfung durchzuführen. Diese Option wechselt zwischen **Ordner prüfen** und **Überprüfung stoppen**. Klicken Sie auf **Überprüfung stoppen**, um die Überprüfung auf Spam-Mails anzuhalten.

Sperren/Zulassen

Hier können Sie E-Mail-Adressen manuell eingeben, die gesperrt oder zugelassen werden sollen. Geben Sie eine E-Mail-Adresse ein, und legen Sie durch Auswahl des betreffenden Optionsfelds fest, ob sie gesperrt oder zugelassen werden soll.

E-Mail-Adresse hinzufügen/entfernen

Im unteren Abschnitt des Dialogfelds ist eine Liste mit E-Mail-Adressen aufgeführt. Beim Eingeben einer neuen Adresse lautet die Standardoption **Sperren**, um die versehentliche Zulassung einer Adresse zu vermeiden, die eigentlich gesperrt sein sollte. Alternativ können Sie aber auch **Zulassen** wählen, wenn Sie E-Mails von diesem Absender empfangen möchten. Die Details in der Liste mit E-Mail-Adressen können Sie jederzeit bearbeiten.

Hinzufügen

Geben Sie eine E-Mail-Adresse ein, z. B.
name1@domain.com.

oder

Geben Sie mehrere durch Komma getrennte E-Mail-Adressen ein, z. B.
name1@domain.com, name2@domain.com.

oder

Geben Sie den Namen einer ganzen Domäne ein, die gesperrt oder zugelassen werden soll, z. B.
phoneysales.com.

Hinweis: Fügen Sie nicht Ihre eigene Domäne hinzu, um „Spoof“-Mails zu vermeiden.

Wählen Sie **Zulassen** oder **Sperren** (Standardoption) für die einzelnen Adressen.

Klicken Sie bei jedem neuen Eintrag auf **Hinzufügen**.

Klicken Sie auf **Speichern**, um neue Adressen oder Domänen aufzubewahren.

Entfernen

Wählen Sie mindestens eine Adresse aus.

Klicken Sie auf **Gewählte entfernen**.

Klicken Sie auf **Speichern**, um die Änderungen zu bestätigen.

Bearbeiten

Wählen Sie mindestens eine Adresse aus.

Geben Sie die gewünschten Änderungen für die E-Mail-Adresse ein, die gesperrt bzw. zugelassen werden soll.

Klicken Sie auf **Speichern**, um die Änderungen zu bestätigen.

Einstellungen

So wie Antiviren-Anwendungen mit Virendefinitionsdateien arbeiten, um Malware zu erkennen, verwenden Antispam-Lösungen Definitionsdateien, um unerwünschte E-Mails herauszufiltern. Virendefinitionsdateien nutzen Virensignaturen, um zu ermitteln, ob eine bestimmte Datei infiziert ist, wohingegen Antispam-Definitionen mithilfe eines bestimmten Kriteriensatzes ermitteln, welche E-Mails vermutlich Spam beinhalten. Spam-Definitionen analysieren E-Mails anhand von Sprache, Bildern, Farben, Hyperlinks, die die Mail enthält, sowie anhand der Absender- und IP-Adresse. Trotzdem lässt sich nicht mit letzter Sicherheit sagen, ob es sich bei einer vorliegenden E-Mail um Spam handelt oder nicht.

Filtergenauigkeit

Wenn Sie mithilfe des Schieberegler die Genauigkeit auf **Niedrig** setzen, untersucht die Antispam-Anwendung nur E-Mails, die extrem verdächtig erscheinen. Infolgedessen werden eher weniger E-Mails als Spam aussortiert. Wenn Sie umgekehrt den Schieberegler auf **Hoch** setzen, sorgt eine breitere Auslegung der Spamkriterien entsprechend für eine größere Anzahl von als Spam aussortierten E-Mails.

Wenn so gut wie kein Zweifel besteht, dass es sich bei einer bestimmten E-Mail um Spam handelt, also wenn sich z. B. der Absender auf der Sperrliste oder in einer Online-Datenbank befindet, wird die E-Mail ungeachtet der Stellung des Schiebereglers blockiert. Wir halten die Standardeinstellung **Mittel** für angemessen zum Ausfiltern unerwünschter E-Mails.

Die Antispam-Filtermethode setzt nie Ihre manuellen Anweisungen bezüglich einer Adresse außer Kraft.

Spamkontrolle konfigurieren

Spamdefinitionen aktualisieren

Hiermit wählen Sie die Häufigkeit für die Aktualisierung der Spamdefinitionen, wobei alle fünf Minuten, einmal täglich oder einmal pro Woche zur Auswahl stehen. Die empfohlene Einstellung ist **Alle fünf Minuten**.

Spamverwaltung

Mithilfe dieser Option bestimmen Sie, wann die vom Spamfilter abgefangenen E-Mails gelöscht werden sollen, und zwar je nach Alter oder Anzahl. Die Standardeinstellungen lauten Alle **Spam-Mails löschen nach** [10] **Tagen** und **Spam löschen, wenn Menge größer als** [500] herausgefilterte E-Mail-Nachrichten ist.

Vergessen Sie nicht, Ihre Änderungen zu bestätigen, indem Sie auf **Speichern** klicken.

Jugendschutz

Öffnen Sie die Einstellungen in der „Security Suite“, und wählen Sie im Menü die Option **Jugendschutz** über den Konfigurationsbutton aus. Nähere Informationen zum Öffnen der Anwendung finden Sie im Abschnitt „Erste Schritte“ in dieser Anleitung.

Ursprünglicher Zugriff

Bevor Sie diese Anwendung zum ersten Mal verwenden, erscheint die Mitteilung *„Administrator nicht erstellt!“* im Start-Dialogfeld, und ein gelbes Warndreieck erscheint auf dem Menüeintrag der Anwendung.

Administrator nicht erstellt

Sie müssen zunächst einen Benutzer mit Administratorrechten ausstatten, um auf diese Anwendung zuzugreifen. Geben Sie ein Kennwort ein, und wählen Sie das Standardprofil. Klicken Sie auf **Speichern**, um fortzufahren.

Das Standardprofil sollte dem am niedrigsten eingestuften Benutzerprofil entsprechen, das eingerichtet werden soll. Wenn Sie also beispielsweise beabsichtigen, ein Kinderprofil einzurichten, sollte das Grundprofil dem Kinderprofil entsprechen. Nur der Administrator darf in der Lage sein, die Benutzer zu bearbeiten und ihre Einstellungen zu konfigurieren, also etwa das Zeitfenster für den Internetzugriff festzulegen und Sperr-/Zulassungslisten zu erstellen. Normalerweise handelt es sich beim Administrator um ein Elternteil.

Diese Einstellungen können Sie auch später noch ändern.

HINWEIS: Das Administratorkennwort kann nicht zurückgesetzt werden. Achten Sie also darauf, dass Sie Ihr Kennwort nicht vergessen. Beim Kennwort ist die Groß-/Kleinschreibung zu beachten.

Administratoranmeldung

Wenn ein Administratorbenutzer erstellt wird, erscheint der Anmeldungsbildschirm. Melden Sie sich mit dem Benutzernamen und Kennwort des Administrators an, um auf die Anwendung zuzugreifen.

Taskleisten-Symbol

Ein Taskleisten-Symbol zeigt an, dass die Jugendschutz Komponente installiert ist. Wenn Sie mit dem Mauszeiger über das Symbol gehen, wird der Statustext eingeblendet, z. B. „Parental Control: 'Administrator' ist angemeldet“.

Hauptseite

Diese Anwendung sperrt den Zugang zu Websites bestimmter Kategorien, und es schränkt Umfang und Zeitraum des Internetzugriffs für Benutzer ein. Dieses Kapitel behandelt das Erstellen, Konfigurieren und Verwalten von Benutzern sowie das Anzeigen von Protokolldateien und das Programmieren des Internetzugriffs. Melden Sie sich mit dem Benutzernamen und Kennwort des Administrators an, um auf die Anwendung zuzugreifen.

Einstellungen

Klicken Sie auf diese Option, um die Standardwerte zu bearbeiten.

Benutzer

Hiermit erstellen Sie Benutzer und weisen ihnen Benutzerprofile zu. Bestehende Benutzer werden in diesem Dialogfeld mit Namen und zugeordnetem Profil aufgeführt.

Es gibt verschiedene Benutzerprofile: **Erwachsener**, **Teenager**, **Kind**. Das letztgenannte Profil ist sehr eingeschränkt und gestattet lediglich den Zugriff auf solche Websites, die manuell vom Administrator in die Zulassungsliste eingetragen wurden.

Erwachsener	Keine Einschränkungen.

Teenager	Durch Kategoriefilter eingeschränkter Zugriff.
Kind	Vollständig eingeschränkt.

Kategorien

Kategorien basieren auf einer Vielzahl von Begriffen und Ausdrücken, anhand derer die Anwendung eine Webseite z. B. als vorrangig erotikorientiert erkennen kann. Die Bedingungen selbst können weder eingesehen noch bearbeitet werden. Für das Profil „Teenager“ gibt es vier Kategorien, die den Zugang zu Webseiten mit dem Inhalt **Erotik**, **Glücksspiel**, **Waffen** und **Drogen** sperren. Alle Kategorien sind standardmäßig aktiviert, aber der Administrator kann die Kategorien deaktivieren, die zulässig sein sollen.

Sperr-/Zulassungsliste

Für Benutzer mit dem Profil „Kind“ muss eine Zulassungsliste eingerichtet werden, da nur die Webadressen auf dieser Liste besucht werden können. Für Benutzer mit dem Profil „Teenager“ können optional Sperr- wie Zulassungslisten eingerichtet werden.

Format der Webadressen

Der technische Begriff für eine Webadresse lautet URL (Uniform Resource Locator). Platzhalterzeichen (*/?) werden in Webadressen nicht unterstützt. Zulässige Formate:

http://www.newspaper.com
www.newspaper.com
newspaper.com

Die Eingabe einer bestimmten Website ermöglicht Ihnen zwar den Zugriff auf die nachgeordnete Domänenebene(n), aber nicht auf die übergeordnete(n) Ebene(n). So würde beispielsweise die Zulassung von www.newspaper.com/kidsstuff keinen Zugriff auf die übergeordnete Ebene www.newspaper.com. Wenn jedoch zeitung.de hinzugefügt wird, sind sämtliche Ebenen dieser Webadresse freigegeben, also etwa news.newspaper.com, cartoon.newspaper.com, usw.

> **HINWEIS: Wenn ein Benutzer einem Link von einer zugelassenen Seite aus folgt, wird dieses zugelassen, egal wohin der Benutzer weitergeleitet wird. Allerdings ist es nicht möglich, eine weitere Seite zu öffnen, es sei denn, dies ist der weiterleitenden Instanz explizit gestattet.**

Standardprofileinstellungen

Das Profil **Erwachsener** hat keine Einschränkungen. Die Profile **Kind** und **Teenager** unterliegen Einschränkungen, die Sie konfigurieren können. Wenn Sie einem Benutzer das Profil **Kind** zuweisen, hat der Benutzer überhaupt nur Internetzugriff, wenn eine Positivliste zugelassener Websites erstellt wurde. Diese einzelnen Profileinstellungen gelten jeweils für alle Benutzer mit dem betreffenden Benutzerprofil.

Standardprofil ‚Kind‘

Bitte beachten Sie, dass Veränderungen an diesem Standardprofil sich auf alle Profilmitglieder auswirken, nicht nur auf einen einzelnen Benutzer. Da für das Profil „Kind“ alle Webseiten blockiert sind, sofern sie nicht ausdrücklich zugelassen werden, gibt es für dieses Profil keine Blockierliste bzw. Kategorie.

Hinzufügen

Geben Sie eine Webadresse, die zugelassen werden soll, im Dialogfeld **Adresse zur Liste hinzufügen** ein.

Falls Sie mehrere Adressen eingeben, trennen Sie diese durch ein Komma.

Klicken Sie bei jedem neuen Eintrag auf **Hinzufügen**.

Entfernen

Wählen Sie mindestens eine Adresse aus.

Klicken Sie auf **Gewählte entfernen**.

Standardprofil ‚Teenager‘

Bitte beachten Sie, dass Veränderungen an diesem Standardprofil sich auf alle Profilmitglieder auswirken, nicht nur auf einen einzelnen Benutzer. Für dieses Profil werden Websites nach Kategorien und Sperr-/Zulassungsliste eingeschränkt.

Kategorien

Standardmäßig sind alle Kategorien ausgewählt, d. h., Websites mit bestimmten Inhalten werden für das Profil „Teenager“ gemäß diesen Einstellungen gesperrt. Die Kategorien sind Erotik, Glücksspiele, Waffen und Drogen. Der Administrator kann die Kategorien einzeln deaktivieren, um Websites der betreffenden Kategorie zuzulassen. Alternativ können Sie Websites auch auf die Zulassungsliste setzen. Klicken Sie auf **Speichern**, um die Änderungen zu bestätigen.

Sperr-/Zulassungsliste

Websites für das Profil „Teenager“ werden gemäß den Einstellungen in den Kategorien gesperrt. Sie können eine oder mehrere Websites hinzufügen, um Zugriff auf einzelne Internetseiten zuzulassen, die sonst einer gesperrten Kategorie angehören würden.

Hinzufügen

Geben Sie eine Webadresse, die zugelassen werden soll, im Dialogfeld **Adresse zur Liste hinzufügen** ein.

Falls Sie mehrere Adressen eingeben, trennen Sie diese durch ein Komma.

Klicken Sie bei jedem neuen Eintrag auf **Hinzufügen**.

Wählen Sie zwischen den Optionen **Sperren** und **zulassen**.

Klicken Sie bei jedem neuen Eintrag auf **Hinzufügen**.

Benutzer anlegen

Wählen Sie die Option **Hinzufügen** im Menü **Einstellungen – Jugendschutz - Benutzer**

Geben Sie einen Namen für den neuen Benutzer ein sowie ein Kennwort, das Sie anschließend bestätigen müssen.

Der nächste Schritt besteht aus dem **Wählen des Standardprofils** für den neuen Benutzer**.**

Sie können zusätzlich dem Profil auch ein Windows Systembenutzer zuordnen.

Mit der Zuordnung eines Profils legen Sie fest, welche Art von Websites der betreffende Benutzer aufrufen kann:

Erwachsener
Keine Einschränkungen. Der Benutzer kann auf alle Websites zugreifen.

Teenager
Grundsätzlich keine Einschränkungen. Allerdings werden Websites mit unerwünschten Themen oder Inhalten durch die Standardeinstellungen der Kategorien gesperrt.

Kind
Nur Zugriff auf die Webseiten, die der Administrator in die Zulassungsliste einträgt.

Klicken Sie auf **Erstellen**, um Ihre Änderungen zu bestätigen.

Der neue Benutzer wird zur Benutzerliste hinzugefügt. Klicken Sie auf einen Benutzernamen, um den betreffenden Benutzer zu konfigurieren.

Kennwort ändern

Geben Sie den Benutzernamen und das Kennwort für den neuen Benutzer ein.

Kategorien

Diese Auswahl steht nur für das Benutzerprofil „Teenager“ zur Verfügung. Um eine oder mehrere Kategorien für einen bestimmten Benutzer mit dem Teenager-Profil zuzulassen, deaktivieren Sie das bzw. die entsprechenden Kontrollkästchen.

Sperr-/Zulassungsliste

Diese Auswahl steht nur für das Benutzerprofil „Teenager" zur Verfügung. Hier können Sie Webadressen für Benutzer zulassen oder sperren.

Zulassungsliste

Diese Auswahl steht für das Benutzerprofil „Kind" zur Verfügung. Hier können Sie Webadressen für Benutzer zulassen.

Zugriffsplaner

Der Administrator kann entscheiden, zu welcher Tageszeit und an welchen Wochentagen Benutzer im Internet surfen dürfen. Die Standardeinstellung sieht keine zeitlichen Einschränkungen vor (grün).

Um den Internetzugriff für einen bestimmten Zeitraum zu sperren, setzen Sie den Cursor auf Tag und Uhrzeit Ihrer Wahl und drücken die linke Maustaste.

Wenn Sie den gesperrten Zeitraum erweitern möchten, ziehen Sie den Cursor entsprechend nach oben/unten bzw. nach rechts/links. Analog dazu können Sie den Status durch Klicken und Ziehen des Cursors von **Verweigern** (grau) in **Zulassen** (grün) ändern.

Klicken Sie auf **Speichern**, um Ihre Änderungen zu bestätigen.

Einstellungen

Es wird automatisch vermieden, dass ein Kind auf einen unbeaufsichtigten Computer zugreift, auf dem ein Erwachsener angemeldet ist (und vergessen hat, sich abzumelden, oder den Computer plötzlich verlassen musste). Nach einer fest eingestellten Leerlaufzeit wechselt der Computer in das Standardprofil.

Profile festlegen

Als Profil, in das die Anwendung nach der festgelegten Dauer zurückgesetzt werden soll, können Sie „Kind" oder „Teenager" angeben.

Kind

Alle Webseiten außer der manuell eingegebenen werden für das Profil „Kind" gesperrt. Dies bedeutet, dass der Internetzugriff überhaupt erst möglich ist, wenn Sie eine Positivliste von Websites für das Benutzerprofil „Kind" festgelegt haben.

Teenager

Webseiten mit bestimmten Inhalten sind gemäß den Einstellungen unter „Kategorien" (Erotik, Glücksspiel, Waffen und Drogen) für das Profil „Teenager" gesperrt.

Einstellungen oder Änderungen werden automatisch übernommen.

Administratorkennwort ändern

Das Administratorkennwort kann zwar nicht zurückgesetzt, aber geändert werden, sofern Ihnen das aktuelle Kennwort bekannt ist. Wenn Sie ein neues Administratorkennwort festlegen, schreiben Sie es am besten auf und verwahren es an einem sicheren Ort.

> **HINWEIS: Achten Sie beim Kennwort auf die Groß-/Kleinschreibung.**

Datenschutztools

Öffnen Sie die Anwendung „Security Suite“, und wechseln Sie in das Einstellungen Menü. Klicken Sie bei der Option **Datenschutztools auf das Konfigurationsicon:** .

Mithilfe dieser Anwendung können Sie bestimmte Dateien sicher löschen. Die Inhalte solcher Dateien sind dauerhaft gelöscht und lassen sich nicht wiederherstellen. Sie können die Anwendung auch so konfigurieren, dass diverse Protokolldateien mit persönlichen Daten, Cookies und Browserverläufen automatisch gelöscht werden. Das Löschen von Verlaufsprotokollen wirkt sich nicht auf die Einstellungen und Lesezeichen einer Anwendung aus.

Programmverlauf eines Benutzers löschen

Die Liste der Benutzernamen zeigt alle registrierten Benutzer des betreffenden Computers an, und die Programmliste zeigt alle Anwendungen an, deren Verlaufsprotokolle Sie löschen können.

Wählen Sie mindestens einen Benutzernamen sowie die Programme aus, deren Verläufe gelöscht werden sollen.

Klicken Sie zum Bestätigen auf **Speichern**

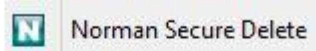
Sicher löschen

Mithilfe dieser Anwendung können Sie bestimmte Dateien sicher löschen. Die Inhalte solcher Dateien sind dauerhaft gelöscht und lassen sich nicht wiederherstellen.

Sie können den Vorgang zum sicheren Löschen von Dateien einleiten, indem Sie einfach mit der rechten Maustaste die betreffende Datei im Windows Explorer anklicken. Sie werden aufgefordert, den Löschvorgang zu bestätigen. Der Löschvorgang wird angezeigt, und nach seinem Abschluss erscheint eine Zusammenfassung. Verfahren Sie folgendermaßen, um Dateien sicher zu löschen:

Wählen Sie mindestens eine Datei aus, die gelöscht werden soll.

Klicken Sie mit der rechten Maustaste die Datei(en) an.

Wählen Sie im Popup-Menü die Option **Norman Secure Delete** aus: 

Klicken Sie zum Bestätigen auf **OK**.

Klicken Sie auf **OK**, um das Dialogfeld „Zusammenfassung“ zu schließen.

Damit sind die betreffenden Dateiinhalte dauerhaft von Ihrem Computer gelöscht.

> **HINWEIS: Das Löschen von Dateien über die sichere Methode ist sehr viel zeitaufwendiger als das normale Löschen von Dateien. Dies liegt daran, dass jeder Dateiteil mehrfach überschrieben wird, um zu verhindern, dass Fragmente der ursprünglichen Inhalte wiederhergestellt werden können.**

Falls Sie den Löschvorgang vorzeitig abbrechen, wird die Datei zwar trotzdem vernichtet, aber nicht so gründlich wie vorgesehen.

Nicht alle Dateien lassen sich löschen. Das liegt entweder daran, dass der Benutzer nicht die erforderlichen Rechte zum Überschreiben der Datei(en) hat oder es sich um geschützte Systemdateien handelt, die von Secure Delete nicht gelöscht werden können.

Eindringschutz (Englisch Intrusion Guard)

Öffnen Sie die Anwendung „Security Suite“, und wechseln Sie in das Einstellungen Menü. Klicken Sie bei der Option



Eindringschutz auf das Konfigurationsicon**:** .

Hauptseite



Bei dieser Anwendung handelt es sich um ein hostbasiertes Angriffsverteidigungssystem (HIPS) für erfahrene Benutzer. Unerfahrene Benutzer sollten die empfohlenen Konfigurationseinstellungen unverändert beibehalten, die hauptsächlich dem Zulassen und Protokollieren von Ereignissen dienen. Hochriskante Ereignisse, die von zulässigen Anwendungen kaum verwendet werden, sind standardmäßig gesperrt.

> **HINWEIS: Es wird dringend empfohlen, dass nur fortgeschrittene Benutzer die Standardeinstellungen ändern.**

Treiber und Speicher

Treiber sind Computerprogramme, die auf einer unteren Ebene ausgeführt werden, der „Kernel-Ebene“. Treiber werden normalerweise für den Zugriff und die Steuerung von Hardware geschrieben, z. B. Monitor, Tastatur, Drucker und Netzwerkkarte. Um auf die an den Computer angeschlossene Hardware zuzugreifen, benötigen Treiber uneingeschränkten Systemzugriff. Daher kommen beim Schreiben bösartiger Anwendungen die gleichen Methoden zum Einsatz. Sie können die Konfiguration der Treiberinstallation ändern, um zu steuern, welche Anwendungen Treiber auf Ihrem Computer installieren dürfen.

Es gibt zwei bösartige Methoden, um die gleichen Rechte wie Treiber zu erlangen. Beide Methoden umgehen den Sicherheitsmechanismus des Betriebssystems. Es wird dringend empfohlen, die Einstellungen in beiden Fällen auf **Verweigern** zu belassen.

Eingabeaufforderung
Sie werden bei jedem Versuch zum Bestätigen aufgefordert.

Zulassen
Versuche werden nur protokolliert.

Verweigern
Keine Anwendung, ob berechtigt oder bösartig, kann Treiber auf der Kernel-Ebene installieren.

Prozesse

Eine auf Ihrem Computer installierte Anwendung – egal ob legitim oder bösartig – wird meist versuchen, automatisch zu starten, sobald der Computer hochfährt. Ein Programm, das automatisch zu starten versucht, kann das Betriebssystem anweisen, automatisch mit den gleichen Rechten wie der aktuelle Benutzer zu starten, wenn der Computer hochfährt. Oder es kann einen Hintergrunddienst installieren, der mit erhöhten Zugriffsrechten ausgeführt wird. Eine Angriffsverteidigungsanwendung kann Zugriffsversuche dieser Art verhindern.

Eingabeaufforderung
Sie werden bei jedem Versuch zum Bestätigen aufgefordert.

Verweigern
Keine Anwendung, ob berechtigt oder bösartig, kann automatisch starten, wenn der Computer hochfährt.

Programme können auch Code in andere Prozesse einschleusen, die auf Ihrem Computer ausgeführt werden, oder Prozesse auf andere Weise missbrauchen. Es handelt sich um das normale Verhalten von bösartigen Anwendungen, allerdings verwenden auch bestimmte zulässige Programme diese Methoden, etwa um das Benutzerdesktop to erweitern oder sonstige erweiterte Funktionen des Betriebssystems oder von Drittanwendungen bereitzustellen. Sie können die Anwendung so konfigurieren, dass jeglicher Versuch verweigert oder Ihnen zur Bestätigung vorgelegt wird.

Sie können eine Liste vertrauenswürdiger Anwendungen so bearbeiten, dass sie zulässige Anwendungen mit ähnlichem Verhalten beinhalten.

Vertrauenswürdige Prozesse

Hier sehen Sie die Liste der Prozesse, welche vom Eindringschutz als solche behandelt werden. Prozesse, welche durch eine Firewall manuell hinzugefügt wurden, können aus der Liste gelöscht werden.

Netzwerk

Indem Sie Filter zu Netzwerkmodulen in Ihrem Betriebssystem hinzufügen, können bösartige Anwendungen persönliche Daten stehlen, z. B. Sozialversicherungsnummern, Kreditkartenangaben und Kennwörter. Adware kann die Netzwerkdaten verändern, die durch solche Filter gesendet werden. So lassen sich die Ergebnisse von Suchmaschinen manipulieren, sodass auf Ihrem Desktop oder auf den von Ihnen besuchten Websites unerwünschte Werbung erscheint.

Unter einem BHO (Browser Helper Object) versteht man eine Erweiterung des Microsoft Internet Explorers. Diese und andere Arten von Plug-ins für den Internet Explorer, z. B. Systemleisten, haben volle Kontrolle über den Netzwerkverkehr zum und vom Internet Explorer, und sie interagieren mit der Benutzeroberfläche.

Bei einem LSP (Layered Service Provider) handelt sich um einen generischen Filter im Netzwerkstapel in Windows. Er hat vollständige Kontrolle über sämtlichen Netzwerkverkehr auf Ihrem Computer.

Wenn Sie eine Website mittels des Domain-Namens (der "Webadresse") aufrufen, wird dieser zunächst in eine IP-Adresse übersetzt. Anschließend werden mit dem entfernten Server Daten ausgetauscht. Ihr Computer schlägt dabei zunächst den Domain-Namen in der Datei „HOSTS“ nach. Dies bedeutet, dass dort vorhandene Einträge jede IP-Adresse überschreiben, die für den Namen geliefert wird. Bösartige Anwendungen können die Datei „HOSTS“ ändern und somit den Netzwerkverkehr auf eine bösartige Website umleiten (sogenanntes „Pharming“).

Eingabeaufforderung

Sie werden bei jedem Versuch aufgefordert zu bestätigen.

Verweigern
Es werden alle Versuche unterbunden, Ihr System zu ändern und ein BHO oder einen LSP zu installieren.

Softwareupdate

Öffnen Sie die Einstellungen Oberfläche der Security Suite, dort können Sie das Intervall der Software Aktualisierung einstellen:



Im Beispiel oben wird also alle 2 Stunden ein Internet Update durchgeführt, um zu prüfen ob neue Signatur oder Programmupdates auf den Norman Servern vorhanden sind.

Proxy eintragen:

Ein Proxy-Server ist ein Computer, der zwischen den Computer des Benutzers und das Internet geschaltet ist. Dieser kann dazu dienen, die Internetnutzung zu protokollieren und den Zugriff auf bestimmte Websites zu sperren. Ferner kann die Firewall des Proxy-Servers dazu verwendet werden, den Zugriff auf bestimmte Seiten von Websites zu sperren.

Falls Ihr Computer von einer Firewall oder einem Proxy-Server geschützt wird, müssen Sie die notwendigen Proxy-Informationen eingeben.

Über den Konfigurationsbutton  können Sie einen Proxy eintragen

Produktsprache auswählen

Sie können die im Zuge der Installation gewählte Sprache ändern. Wählen Sie im Einstellungen Menü unter dem Punkt **Sprache:**



die gewünschte Sprache aus, und bestätigen Sie dieses anschließend mit OK. Die Änderungen werden mit der nächsten Aktualisierung wirksam.

Lizenzassistent (Lizenz eintragen)

Der Lizenzassistent prüft und aktualisiert die Lizenz.

Über den Button „Lizenz aktualisieren" im „Einstellungen" Menu der Security Suite:

Lizenz | Lizenz aktualisieren | Läuft ab in 11 Monaten

können Sie den Norman Lizenzassistenten öffnen. Wenn Sie diese Option wählen, erscheint ein Dialog mit Informationen zu den installierten Produkten und Lizenzschlüsselinformationen. Sie benötigen einen gültigen Schlüssel, um die Installation zu aktualisieren.

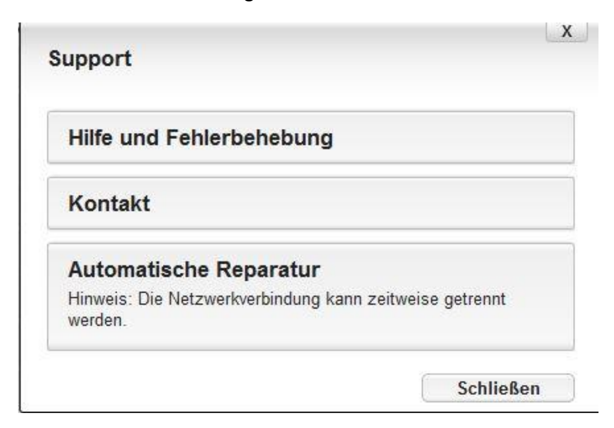
Hier können Sie z.B. auch den Lizenzschlüssel neu eintragen, sollten Sie eine neue Lizenz für eine bestehende Installation erworben haben. Sollte sich der Lizenzassistent über den o.a. Button nicht starten, folgen Sie diesen Schritten:

Bei einer Verlängerung der Lizenz und bereits installiertem Norman Produkt, können Sie den Lizenzschlüssel einfach über den Lizenz Wizard eintragen. Es ist nicht notwendig das Produkt neu zu installieren. Es wird sich automatisch aktualisieren.

Der Lizenz Wizard (LicWiz.exe) befindet sich im ...\Norman\Npm\Bin Verzeichnis (z.B. c:\programme\norman\npm\bin). Starten Sie die LicWiz.exe in dem genannten Verzeichnis und tragen Sie Ihren Lizenzschlüssel dort ein, Nun führen Sie ein Internet Update aus, damit der neue Schlüssel validiert wird.

Support Center

Öffnen Sie die Anwendung „Security Suite“, und wählen Sie im linken Menü die Option **Support** aus. Es öffnet sich anschließend folgendes Bild:



Das **Support Center** liefert Informationen, wo Sie weitergehende Hilfe erhalten, als sie die Produktdokumentation und Onlinehilfe bietet. Ferner finden Sie hier eine automatische Reparaturfunktion, die nützlich sein kann, falls Probleme mit der installierten Software auftreten.

Hilfe und Fehlerbehebung

Wenn Sie auf den Link **Hilfe und Fehlerbehebung** klicken, rufen Sie die Website von Norman auf. Dort finden Sie eine Vielzahl hilfreicher Materialien, die Ihnen in den meisten Fällen helfen werden. So finden sie auf dieser Website z. B.:

Support

Security Center

das Support Forum von Norman

Wenn auch das Durchsuchen dieser Ressourcen keine Abhilfe schafft, wenden Sie sich bitte an Ihren Vertragshändler oder direkt an die nächste Norman-Niederlassung.

Kontakt

Auf dieser Seite finden Sie Telefonnummern und Adressen, über die Sie sich an Ihre zuständige Norman-Niederlassung wenden können. Diese Informationen finden Sie auch auf der letzten Seite des vorliegenden Dokuments.

Automatische Reparatur

Wenn bei der installierten Version der Security Suite Probleme auftreten, können Sie jederzeit probehalber eine automatische Reparatur durchführen lassen, bevor Sie sich an den Kundendienst wenden.

Wenn Sie auf **Automatische Reparatur** klicken, wird im Hintergrund ein Vorgang gestartet, bei dem Ihre Installation geprüft und ggf. Dateien oder Komponenten aktualisiert werden. Während der Durchführung der automatischen Reparatur wird im Taskleistenmenü das Zahnsymbol angezeigt. Eine Erläuterung der Taskleistensymbole, die für die Security Suite von Bedeutung sind, finden Sie auf Seite <?>.

Wenn Sie keinen Zugriff auf die Benutzeroberfläche haben, können Sie über c:\Programme\Norman\nvc\bin die Datei delnvc5.exe starten und die Option **Reparieren** wählen.

NSS deinstallieren

Es gibt zwei Methoden, Norman Security Suite zu deinstallieren. Eine verwendet die Windows-Funktion **Programme hinzufügen/entfernen**. Die andere verwendet das Deinstallationsprogramm von Norman.

Verfahren Sie folgendermaßen, wenn Sie über das Windows-Betriebssystem vorgehen möchten:

Gehen Sie nacheinander auf **Start > Systemsteuerung > Programme hinzufügen/entfernen**.

Wählen Sie unter Vista / 7 / 8 **Programme und Funktionen**.

Führen Sie einen Bildlauf bis zur Anwendung „Norman“ aus, und markieren Sie diese.

Wählen Sie die Option **Entfernen**.

Nach der Deinstallation des Programms starten Sie den Computer neu.

Verfahren Sie folgendermaßen, wenn Sie das Deinstallationsprogramm von Norman verwenden möchten:

Gehen Sie nacheinander auf **Start > Ausführen**, und geben Sie den Dateipfad zu delnvc5.exe ein.

Der Standardpfad lautet C:\Programme\Norman\nvc\bin\delnvc5.exe.

Wählen Sie die Option **Entfernen**.

Führen Sie nach entsprechender Aufforderung einen Neustart des Computers durch.

Anhang A

Was ist eine Sandbox?

Als Sandbox wird die Technik bezeichnet, mit der eine Datei auf unbekannte Viren untersucht wird. Der Name wurde bewusst gewählt, denn das Verfahren lässt zu, dass nicht vertrauenswürdiger, möglicherweise mit Viren infizierter Code auf dem Computer ausgeführt wird – allerdings nicht auf dem realen Computer, sondern in einem simulierten und abgegrenzten Bereich. Die Sandbox enthält alles, was ein Virus auf einem realen Computer erwartet. Auf diesem „Spielplatz" kann sich der Virus replizieren, ohne Schaden anzurichten. Jeder Schritt wird überwacht und protokolliert. In der Sandbox wird der Virus entlarvt. Da alle seine Aktionen aufgezeichnet werden, kann automatisch ein Gegenmittel für diesen neuen Eindringling erzeugt werden.

Ein moderner E-Mail-Wurm kann innerhalb von Sekunden Zehntausende von Workstations infizieren. Die Sandbox-Funktion von Norman kann sich als wertvolles Werkzeug für das „Einfangen" neuen zerstörerischen Codes erweisen.